ID01120001
Attachment 7

C. PERFORMANCE WORK STATEMENT

1.0. INTRODUCTION

This Alliant GWAC Task Order supports the Department of Housing and Urban Development Office of the Inspector General Information Systems Division (HUD OIG ISD). The work described in this Performance Work Statement (PWS) includes the contract scope and objectives, operation, support, and maintenance of the HUD OIG ISD Distributed Computing Environment (DCE).

2.0. SCOPE AND OBJECTIVE

2.1. SCOPE

This Task Order provides operations and maintenance support for the HUD OIG ISD Distributed Computing Environment (DCE) to accomplish the following mission critical services in accordance with all Federal rules, regulations and policies:

- Supporting, maintaining and deploying DCE equipment located in the Central Server Facility (CSF) and Disaster Recovery Facility (DRF).
- Supporting, maintaining, and deploying all Office of the Chief Information Officer (OCIO) approved local area networks (LANs) at HUD OIG locations.
- Supporting and maintaining the end-user workstation. The end-user workstation includes a laptop computer, laptop docking station, a flat screen monitor, a keyboard, and a mouse.
- Supporting and maintaining other end-user network-connected hardware (desktops, video conferencing equipment, printers, and scanners).
- Supporting and maintaining the hardware for the custom-built application infrastructure.
- Supporting, maintaining, and monitoring security for the infrastructure and applications including data and databases.
- Providing end-user support across the HUD OIG ISD infrastructure.
- Performing DCE operations and maintenance (e.g., backups, routine maintenance).
- Providing and maintaining updated documentation for DCE according to industry standard configuration management practices.

The Contractor shall furnish the necessary personnel, materials, equipment, software, telecommunications, facilities and related services required to perform this Contract. The Contractor is not responsible for

- Supporting and provisioning of phone lines and service.
- Hosting, supporting and maintaining the Central Server Facility
- Hosting, supporting and maintaining the Disaster Recovery Facility
- Deploying the wide-area network (WAN).

2.2. OBJECTIVES

HUD OIG ISD's overarching objective is to have a robust and secure, nationwide and enterprise-wide information technology infrastructure that complies with Federal rules, regulations, and policies and helps it accomplish its mission. The Contractor shall meet the following objectives:

- Configure server and network resources to ensure that all locations meet or exceed response times as defined in the attached Technical Performance Index (TPI) (Attachment 8)
- Where appropriate, incorporate innovative and emerging technologies that improve infrastructure and mission performance while providing the best value to the government.
- Contractor support to end users as specified in the TPI.
- Provide, deploy, and maintain HUD OIG ISD approved hardware.

3.0. HUD OIG ORGANIZATION

3.1. BACKGROUND

The HUD OIG is a semi-autonomous operational organization within HUD that was authorized with the signing of the Inspector General Act of 1978 (Public law 95-452). The Inspector General (IG) has the authority to inquire into all of the programs and administrative activities of the Department. The HUD OIG serves its customers by being a proactive force in identifying and mitigating problems while remaining committed to its statutory mission of identifying and preventing waste, fraud, and abuse and promoting the effectiveness and efficiency in the Department's programs, activities, and functions. The HUD OIG receives and processes complaints of inappropriate behavior or violations of law; conducts audits and investigations of HUD activities; and develops, analyzes, and reviews legislative and policy proposals.

The HUD OIG's mission is independent and objective reporting to the Secretary and the Congress for the purpose of bringing about positive change in the integrity, efficiency, and effectiveness of HUD operations.

The HUD OIG consists of four distinct organizational units, each subsisting under different authorities and sets of responsibilities:

- Office of Audit (OA): The OA is responsible for planning and conducting audits of departmental activities that include: (a) HUD headquarters and field operations, (b) programs and initiatives, and (c) contractors and other entities doing business with the Department. The OA workload can be sectioned into three general categories: performance audits, financial audits, and advisory and assistance services.
- Office of Investigation (OI): The OI is responsible for the development and implementation of the Department's investigative activities. These activities are performed by personnel located at HUD Headquarters and in the field offices. The Office initiates investigations of possible violations of laws or regulations in the administration of the HUD programs and activities or the misconduct on part of the HUD employees.
- Office of Management and Policy (OMAP): The OMAP provides HUD OIG-wide administrative support and is responsible for human resources, information systems management, automated office support services, budget and financial management,

contract support, employee training, internal policy development, records management, reports, and quality control.

The HUD OIG Hotline is the central complaint intake operation for HUD OIG. The mission of the HUD OIG Hotline is to take, manage, and address reports of violations of law, rules, or regulations and allegations of waste, fraud, abuse or mismanagement

- Office of Legal Counsel (OLC): The OLC is responsible for independently providing the full range of professional legal services and advice with respect to the formation, revision, and execution of the entire HUD OIG program.

3.2. STAFF AND FACILITIES

Approximately 750 HUD OIG staff from the four organizational units are located throughout the United States, Puerto Rico, and Territories. Each of these locations is covered under this contract. The list of locations and the approximate numbers of staff in each location (as of September 1, 2010) are listed below.

Table 1 - HUD OIG Locations

Pacific/Hawaii District – Sacramento, CA – 5 – San Francisco, CA – 11 – Los Angeles, CA – 41 – Phoenix, AZ – 9 – Las Vegas, NV – 5 Southwest District – Fort Worth, TX (INV) – 13 – Ft Worth, TX(AUD) - 14 – Houston, TX – 13 – San Antonio, TX – 8 – Baton Rouge, LA - 1 – New Orleans, LA –17 – Oklahoma City, OK – 6 Great Plains District – Kansas City, KS – 17 – St. Louis, MO – 13 – Northwest/Alaska District – Seattle, WA – 20 Rocky Mountains District	Southeast/Caribbean District – Atlanta, GA - 35 – Birmingham, AL – 3 – Columbia, SC - 2 – Greensboro, NC – 19 – Hattiesburg, MS – 1 – Jackson, MS - 9 – Jacksonville, FL - 6 – Knoxville, TN – 5 – Little Rock, AR – 2 – Louisville, KY – 2 – Memphis, TN - 5 – Nashville, TN - 4 – San Juan, PR - 9 – Tampa, FL - 13 – Miami, FL – 16 New England District – Boston, MA - 25 – Hartford, CT - 8 – Manchester, NH - 3 New York/New Jersey District – New York, NY - 45 – Albany, NY - 3

– Denver, CO - 15 – Billings, MT - 1 – Salt Lake City, UT - 2 <u>Midwest District</u> – Chicago, IL - 50 – Columbus, OH - 9 – Cleveland, OH - 12 – Detroit, MI – 23 – Grand Rapids, MI – 2 – Indianapolis, IN – 3 – Minneapolis-St. Paul, MN – 4	– Buffalo, NY - 6 – Newark, NJ - 17 <u>Mid-Atlantic District</u> – Philadelphia, PA - 30 – Baltimore, MD (INV) – 13 – Baltimore, MD (AUD) – 7 – Pittsburgh, PA - 9 – Richmond, VA - 8 <u>Capital District</u> Washington Field Office - 12 <u>Headquarters</u> – Potomac Center - 26 – Washington, DC (HQ) – 129 (47) – Washington, DC (Hotline) – 16 (included in HQ)

3.3. HOW WORK IS PERFORMED

HUD OIG employees are highly mobile—they conduct audits and criminal investigations in public housing authorities, privately owned multifamily housing projects, and mortgage banking offices around the country. These employees need high-speed access to the DCE from wherever they are working, while maintaining the security of the network and data. Also, HUD OIG managers frequently travel to subordinate offices to review work in progress. It is imperative that the Contractor enable these managers to access the DCE network from an unoccupied workstation in the subordinate office with full access to their own data as if they were at their assigned duty station.

4.0. CURRENT DISTRIBUTED COMPUTING ENVIRONMENT

The existing DCE is made up of the following infrastructure, connectivity and other components:

- Server and network facilities (includes DRF and CSF)
- Connectivity to the HUD IT infrastructure
- HUD OIG office connectivity and infrastructure
- DCE hardware and software (includes workstations/desktops/handhelds)
- Security
- Web environment
- Custom built Software applications (includes corrective and adaptive maintenance)
- Help Desk and end-user support

These items are discussed in the following sections.

4.1. SERVER FACILITIES

4.1.1. THE INTEGRATION AND TEST FACILITY

The Integration and Test Facility tests the predictability and reliability of commercial off-the-shelf (COTS) software as well as patches and software upgrades. The facility also manages patches, new software upgrades and ensures that users always have the most current version. The Integration and Test Facility is set-up to mirror a remote site in order to test software releases prior to production roll-out.

4.1.2. CENTRAL SERVER FACILITY

The current DCE network provides reliable, secure communications between HUD OIG personnel and a Central Server Facility (CSF), the primary repository of data. The CSF is housed in a limited access room within a secure building under guarded and monitored protection 24 hours per day, 7 days per week. The CSF, located in, DC, securely houses all primary servers. In addition, HUD OIG ISD infrastructure elements and critical value-added services, such as e-mail and Web access, are monitored at the CSF. The servers at the CSF are backed up by a storage device and a tape library system. The CSF facility allows HUD OIG clients access to databases and information.

Remote connection to the CSF utilizes a virtual private network (VPN). The laptops are protected by encryption. The CSF connects to the HUD IT Network via DS3 circuits and an authentication server and firewall. The CSF also connects to the National Finance Center, local police departments, and the Justice Department's Justice Consolidated Network for the purpose of accessing NCIC/NLETS.

The Central Server Facility has the following services that are connected to the production network:

- The Central Server Facility houses all production servers and support hardware.
- Back-up and restore software is used to back up HUD OIG data daily, weekly, and monthly. Scheduled backups include incremental and full backups.
- A remote access portal authenticates remote users to the HUD OIG. Once validated by the server, clients are allowed access to resources in the HUD OIG environment.

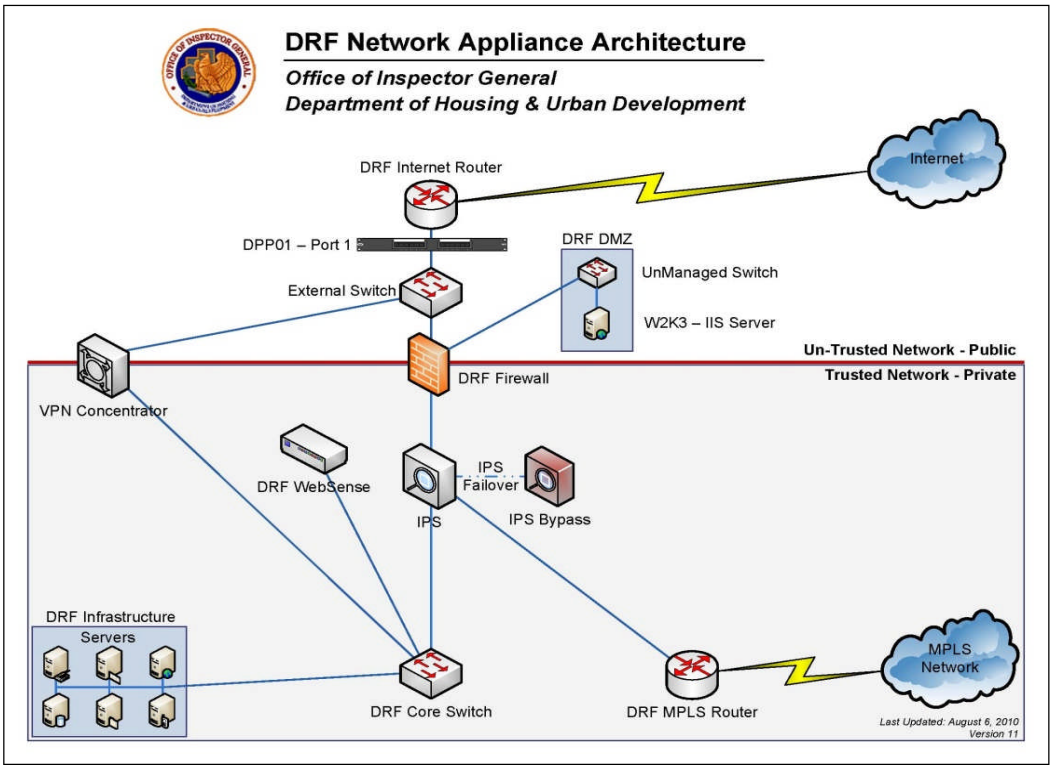
4.1.3. DISASTER RECOVERY FACILITY

In the event the CSF is unreachable, the network will reroute data to the Disaster Recovery Facility (DRF) which will provide full redundancy and operational continuity for HUD OIG ISD identified critical services. The DRF is located in Denver, CO, in a room within a secure building under guarded and monitored protection 24 hours per day, 7 days per week. All DRF equipment is housed in locked equipment enclosures within the designated DRF area. This facility contains standby servers that are continuously updated and can become primary servers when a failure occurs at the CSF.

4.1.4. CSF AND DRF EQUIPMENT AND CONFIGURATION

4.2.

Figure 1 –Architectural Configuration



A high-level diagram of the overall current configuration is presented in Figure 1 above. Both data centers provide simultaneous access to the internet, DNS and Microsoft Active Directory services for Authentication. These hub sites also host VPN connectivity for HUD OIG staff working outside of the office. The VPN provides a secure encrypted tunnel allowing the staff to safely access organizational resources from the internet.

All CSF and DRF support services are accessible via remote consoles. Standard COTS network management tools are in place to both monitor and correct network and server related problems. The Contractor shall furnish sufficiently trained and knowledgeable staff to perform the following activities:

- Monitor, maintain, and sustain healthy operations of all OCIO approved local-area network (LAN) and data center related equipment
- Ensure availability of data, server, and network services to 'three-nines,' e.g., 99.9% uptime
- Support WAN/LAN interfaces

The listing of the current configuration is shown below in Table 2.

Table 2 - CSF and DRF Infrastructure Specifics

Location Name	# of HUD OIG Employees	Infrastructure Hardware	WAN/LAN Telecommunication
Central Server Facility and Central Server Facility Test Office	N/A	Main Infrastructure Systems 69 Enterprise Servers 2 Tape Library Server	1 T3 1 T1
Disaster Recovery Facility	N/A	22 Enterprise Servers	1 T3

A description of the servers in the CSF and DRF is presented below in Table 3:

Table 3 -CSF and DRF Server List

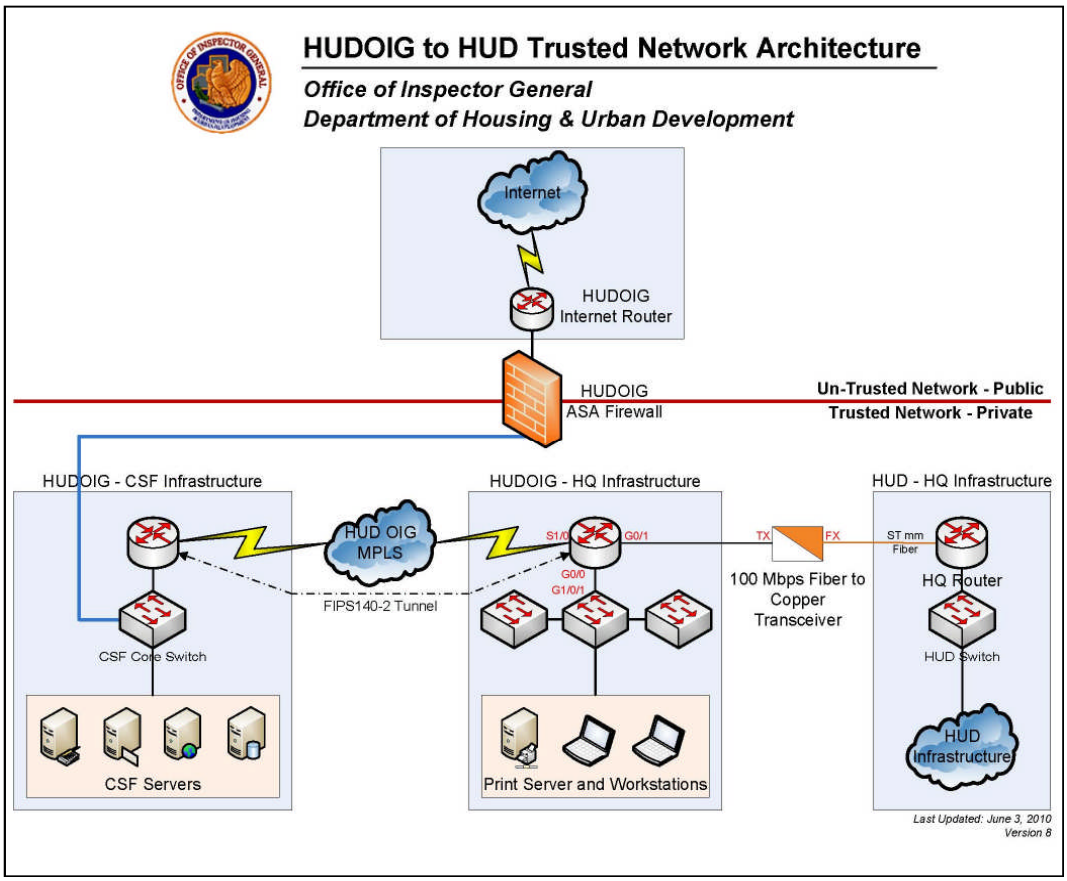
Location	# Servers	Description
CSF	1	Domain Controller
	1	Application Server
	1	Anti-virus Server
	1	Application Server - encryption
	1	Application Server – network management
	2	Backup Server
	1	Blackberry Monitoring Server
	1	Blackberry Enterprise Server
	1	Certificate Authority Server
	1	Remote access Data Source
	1	Remote access Licensing
	7	Remote access App
	2	Remote access Server
	2	Remote access WEB Interface
	1	CMIS Index Server
	1	CMIS Intranet Server
	2	CMIS Database Server
	5	Database Server
	1	DC, DNS 1 DHCP
	1	Fusion Server
	1	HelpDesk Ticketing System Server
	1	HUDShare File Server
	1	Intranet Server
	1	Intrusion Protection Server
	1	ISAD File Server
	1	Email Administrator Server
	1	Email

Location	# Servers	Description
	4	email Application Server
	1	Email Archive Server
	1	Email Demo Server
	2	Email Mail Server
	1	Email Server
	1	Email Web Server
	4	Network Monitoring Server
	1	Router Management Server
	1	SDLT Restore Server
	2	Group Server
	1	Site Protector Server
	4	Utility Server
	1	VPN DHCP
	1	Video Conferencing Server
DRF	1	Backup Server
	1	Blackberry Server
	1	CMIS Server
	1	CMISS Index Server
	3	Database Server
	1	Domain Controller
	1	DMZ-Public Web Server
	1	File Server - HUDSHARE
	1	File Server-Users' Home Directories
	1	Intranet Server
	1	Intrusion Protector Server
	3	Email Application Server
	4	Email Mail Server
	1	Email Web Mail Server
	1	Utility Server

4.2. CONNECTIVITY TO HUD IT INFRASTRUCTURE

The DCE has to maintain a secure connection to the HUD IT environment. Currently, data flows to and from the DCE and the HUD IT environment from the backbone cloud through Verizon. HUD OIG users with access to HUD applications will be required to have an appropriate user id and password to pass through the authentication server. Once authenticated, users will be granted access to required mainframe, secured Internet, and Intranet services. The graphic below depicts the DCE connectivity to HUD IT infrastructure.

Figure 2 - HUDOIG to HUD Trusted Network Architecture

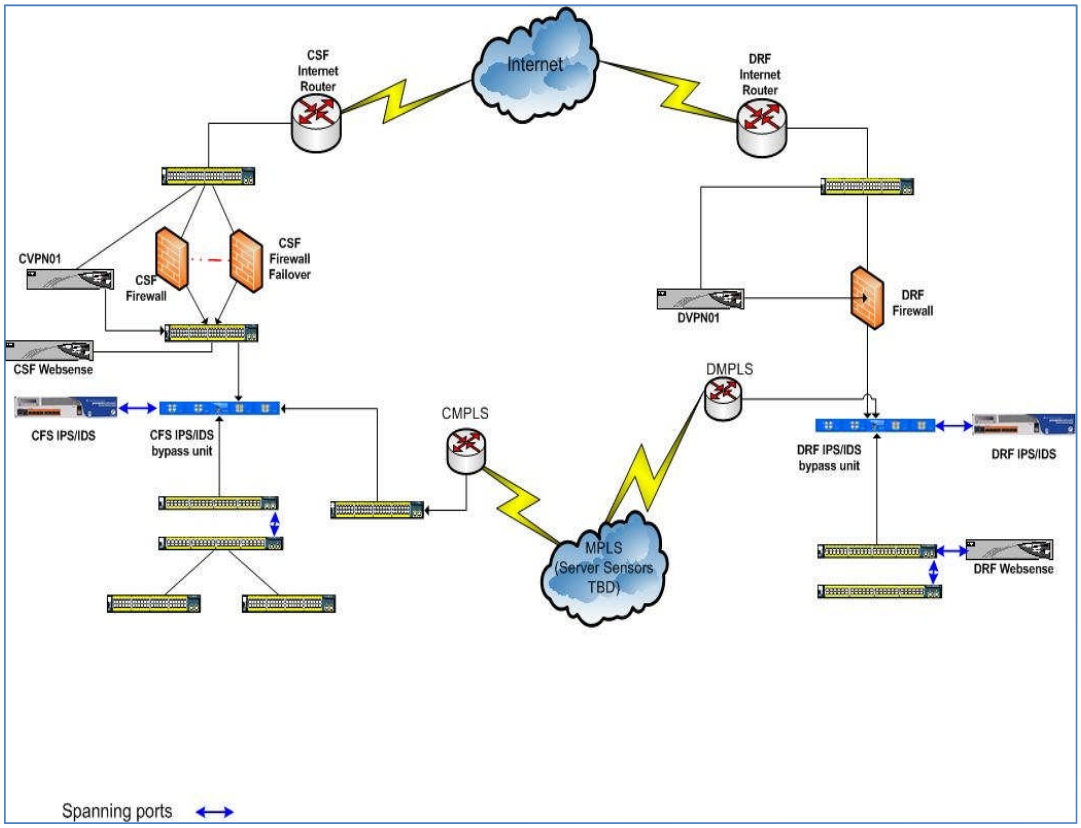


4.3. WIDE AREA NETWORK AND NETWORK OPERATIONS CENTER

4.3.1. DESCRIPTION OF THE WIDE AREA NETWORK

The physical Wide-Area Network (WAN) is maintained under a separate contract. The Contractor is responsible for HUD-OIG owned equipment that directly connect to the WAN. HUD OIG ISD's Wide Area Network (WAN) allows secure encrypted nationwide access to the DCE. The WAN utilizes direct internet access (DIA) and full T-1 through T-3 circuits to connect all HUD OIG locations and users back to the CSF. The communications infrastructure and all equipment are purchased from Verizon by the HUD OIG. A high level description is shown in Figure 3 below.

Figure 3 -Wide Area Network



The HUD OIG ISD network is a hub and spoke topology. The network contains two hubs, the CSF in the eastern portion of the United States and the DRF in the western portion. The branch offices connect to the closest hub for network connectivity and internet access. The furthest hub is used for redundancy in the event the branch office's primary hub becomes unavailable. If a branch office's primary hub goes offline the network will automatically detect the outage and route the traffic to the secondary hub.

The hub and spoke topology is based off the Private IP MPLS offering hosted by Verizon. In addition to the Verizon offering, additional configurations have been implemented to encrypt the traffic that is traveling across the Verizon WAN links for added security and FIPS 140-2 compliance. Both data centers have security measures in place to protect the HUD OIG network from the internet. These security measures include firewalls, intrusion prevention systems, spam filtering appliances and URL filtering mechanisms.

Both data centers provide simultaneous access to the internet, DNS and Microsoft Active Directory services for Authentication. These hub sites also host VPN connectivity for HUD OIG staff that is working out of the office. The VPN provides a secure encrypted tunnel allowing the staff to safely access organizational resources from the internet.

The primary data center located in the eastern portion of the United States is the primary host for all HUD OIG applications and services. The secondary data center in the western portion of the

United States serves as a disaster recovery facility for all mission critical services. These mission critical services include BES for Exchange, CMISS, EDSS, HUDshare, AutoAudit, AutoInvestigations, Hotline and MS Exchange email.

Application access within the data center is load balanced and distributed using specialized load balancing appliances for certain applications. These appliances detect the load and availability on servers and balance application traffic appropriately. If an application is protected by one of these the appliances, the appliance will detect if a service becomes unavailable and automatically redirect traffic to an available server. The applications currently protected by these appliances include Citrix and Office Communication Server. More applications will be added to these appliances in the future.

Looking to the future, HUD OIG ISD is moving towards VMWare to host its Windows computing platform. This platform will host the Windows operating system and cause it to become independent of the hardware. Should the hardware fail, VMWare will detect the problem and automatically migrate the entire operating system to a different hardware platform.

The HUD OIG ISD is in the process of creating a highly available computing platform. Measures are being put in place to detect and correct failures automatically with little or no disruption to the user community. Once the design and implementation of this redundancy mechanism is in place and configured correctly, it will show in increased system availability and end user satisfaction.

4.3.2. NETWORK OPERATIONS CENTER

The Network Operations Center (NOC), operated and managed by a telecommunications vendor, is a state-of-the art, applications resolution support management center using leading edge technology to gain accuracy and efficiency in providing technical support. The NOC manages and monitors HUD OIG ISD's network WAN equipment (routers, VPN gates). The NOC provides the monitoring and management of WAN components to the wiring closets on a per-device basis. It also provides statistical information on the DCE network interface protocol configurations that are reported on a regular basis.

NOC support activities include:

- Documenting WAN performance levels
- Verifying WAN service levels
- Resolving WAN service level problems
- Supporting WAN/LAN interface

4.3.3. VIRTUAL PRIVATE NETWORK (VPN)

The VPN communication paths are used for HUD OIG personnel located in field offices, as well as the roving user who may be connecting from either a hotel room or other remote location. The HUD OIG user located in a fixed field office is provided a VPN connection from the office-level communication rack outward through the Intranet to the gateway located at the CSF. The HUD OIG user dialing in from a mobile location is provided a VPN connection from the laptop through to the gateway at the CSF. In this way all WAN communications are encrypted and protected.

The network further utilizes Windows 2000/2003 servers and provides a hierarchical file system to further enhance security.

4.3.4. LOCAL AREA NETWORK (LAN)

Local Area Network service is furnished via commercial off the shelf Ethernet switches, hubs and routers.

4.4. HUD OIG OFFICE CONNECTIVITY AND INFRASTRUCTURE

Each HUD OIG office is connected to the DCE through the WAN, and each office has some level of DCE infrastructure (e.g., workstations, servers, printers, or desktops). Details on specific installed components, by location, are presented in the following sections.

4.4.1. WASHINGTON, DC OFFICES

The Contractor shall replace and maintain Government Furnished Equipment (GFE) according to the HUD OIG ISD identified schedule. The infrastructure and connectivity specifics for the Washington, DC offices are presented in Table 4 below.

Table 4 - Washington, DC Location Infrastructure Specifics

Location Name	# of HUD OIG Employees	Infrastructure Hardware Specifics	WAN/LAN Telecommunication Specifics
Washington, DC – HQ	150	1 LAN Server 6 LAN Switches 5 Desktops 40 Printers with manufacturer maintenance contracts 1 Workstation per employee	1 T3
Washington, DC – Portals	38	3 LAN Server 3 LAN Switches 1 Server 2 Laser Printers 1 Color Printer 1 Workstation per employee	1 T1 1 T3

4.4.2. MANAGED FIELD OFFICES

A Managed field office is defined as HUD OIG office space where there is at least one server. The list of the managed field offices and the corresponding hardware and telecommunication specifics are presented below in Table 5. The Contractor is responsible for replacing or maintaining the DCE equipment according to the HUD OIG ISD identified schedule

Table 5 - Field Office Infrastructure Specifics

Location Name	# of HUD OIG Employees	Infrastructure Hardware Specifics	WAN/LAN Telecommunication Specifics
Albany, NY	3	1 LAN Server 1 LAN Switch 1 Workstation per employee	1 T1, 128k port
Albuquerque, NM	3	1 LAN Server 1 LAN Switch 1 Multi-function Printer 1 Workstation per employee	1 T1
Atlanta, GA	35	1 LAN Server 2 LAN Switches 1 Desktop 4 Laser Printers 3 Color Printer 1 Workstation per employee 4 Multifunctional Devices	1 fractional T3 (12Mbs)
Baltimore, MD (Investigations)	13	1 LAN Server 1 LAN Switch 2 Desktops 1 Multifunctional Devices 1 Workstation per employee	1 fractional T3 (12Mbs)
Baltimore, MD (Audit)	7	1 LAN Server 1 LAN Switch 1 Multifunctional Devices	1 fractional T3 (12Mbs)
Billings, MT	1	1 LAN Server	1 T1
Boston, MA	25	1 LAN Server 2 LAN Switches 2 Laser Printers 2 Color Printers 2 Multifunctional Devices	1 fractional T3 (12Mbs)
Buffalo, NY	6	1 LAN Server 1 LAN Switch 2 Multifunctional Devices1 Workstation per employee	1 T1

Location Name	# of HUD OIG Employees	Infrastructure Hardware Specifics	WAN/LAN Telecommunication Specifics
Chicago, IL	50	1 LAN Server 4 LAN Switches 1 Desktop 4 GFE Printers 1 GFE Color Printer 3 Laser Printers 1 Color Printers 4 Multifunctional Devices 1 Workstation per employee	1 fractional T3 (12Mbs)
Cleveland, OH	12	1 LAN Server 1 LAN Switch 1 Desktop 1 Color Printer 1 Multifunctional Device 1 Workstation per employee	1 T1
Columbus, OH	9	1 LAN Server 2 LAN Switches 2 Color Printers 3 Laser Printers 2 Multifunctional Device 1 Workstation per employee	1 T1
Denver, CO	15	1 LAN Server 1 LAN Switch 3 Laser Printer 1 Color Printer 2 Multifunctional Device 1 Workstation per employee	1 fractional T3 (12Mbs)
Detroit, MI	23	1 LAN Server 1 LAN Switch 1 Color Printers 2 Multifunctional Device 1 Workstation per employee	1 T1

Location Name	# of HUD OIG Employees	Infrastructure Hardware Specifics	WAN/LAN Telecommunication Specifics
Fort Worth, TX	13	1 LAN Server 1 LAN Switch 2 Laser Printer 2 Multifunctional Device 1 Workstation per employee	1 fractional T3 (12Mbs)
Fort Worth, TX	14	1 LAN Server 1 LAN Switch 2 Laser Printer 1 Color Printer 1 Multifunctional Device 1 Workstation per employee	1 T1
Greensboro, NC	6	1 LAN Server 1 LAN Switch 1 Multifunctional Device 1 Workstation per employee	1 T1
Hartford, CT	8	1 LAN Server 1 LAN Switch 1 Color Printer 1 Laser Printer 3 Multifunctional Devices 1 Workstation per employee	1 T1
Hato Rey (San Juan), PR	9	1 LAN Server 1 LAN Switch 3 Laser Printers 3 Multifunctional Devices 1 Workstation per employee	1 T1
Houston, TX	13	1 LAN Server 2 LAN Switches 1 Desktop 2 Multifunctional Devices 1 Workstation per employee	1 T1
Indianapolis, IN	3	1 Color Printer 1 Workstation per employee	1 T1

Location Name	# of HUD OIG Employees	Infrastructure Hardware Specifics	WAN/LAN Telecommunication Specifics
Jackson, MS	9	1 LAN Server 1 LAN Switch 1 Color Printer 1 Multifunctional Device 1 Workstation per employee	1 T1
Jacksonville, FL	6	1 LAN Server 1 LAN Switch 1 Laser Printer 1 Multifunctional Device 1 Workstation per employee	1 T1
Kansas City, MO	24	1 LAN Server 2 LAN Switches 1 Desktop 1 Laser Printer 2 Color Printers 2 Multifunctional Device 1 Workstation per employee	4 T1
Knoxville, TN	5	1 LAN Server 2 LAN Switches 1 Laser Printer 1 Workstation per employee	1 T1
Las Vegas, NV	5	1 LAN Server 1 LAN Switch 1 Laser Printer 1 Multifunctional Device 1 Workstation per employee	1 T1
Little Rock, AR	2	1 LAN Server 1 LAN Switch 1 Laser Printer 1 Multifunctional Device 1 Workstation per employee	1 T1

Location Name	# of HUD OIG Employees	Infrastructure Hardware Specifics	WAN/LAN Telecommunication Specifics
Los Angeles, CA	41	1 LAN Server 3 LAN Switches 3 Color Printers 5 Laser Printers 2 Multifunctional Devices 1 Workstation per employee	1 fractional T3 (12mbs)
Louisville, KY	2	1 LAN Server 1 Workstation per employee	No Circuit
Manchester, NH	3	1 LAN Server 1 LAN Switch 1 Laser Printer 1 Color Printer 2 Multifunctional Devices 1 Workstation per employee	1 T1
Memphis, TN	5	1 LAN Server (Note 6) 1 LAN Switch 1 Laser Printer 1 Workstation per employee	No Circuit
Miami, FL	16	1 LAN Server 1 LAN Switch 1 Desktop 2 Laser Printers 1 Multifunctional Device 1 Workstation per employee	1 T1
Minneapolis, MN	4	1 LAN Server 1 LAN Switch 1 Laser Printer 1 Workstation per employee	1 T1
New Orleans, LA	17	1 LAN Server 1 LAN Switch 2 Laser Printers 2 Color Printers 2 Multifunctional Devices 1 Workstation per employee	1 T1

Location Name	# of HUD OIG Employees	Infrastructure Hardware Specifics	WAN/LAN Telecommunication Specifics
New York, NY	45	1 LAN Server 2 LAN Switches 1 Desktop 7 Laser Printers 2 Color Printers 2 Multifunctional Devices 1 Workstation per employee	1 fractional T3 (12Mbs)
Newark, NJ	17	1 LAN Server 2 LAN Switches 2 Desktops 2 Laser Printers 1 Color Printer 2 Multifunctional Devices 1 Workstation per employee	1 fractional T3 (12Mbs)
Oklahoma City, OK	6	1 LAN Server 1 LAN Switches 1 Multifunctional Device 1 Workstation per employee	1 T1
Philadelphia, PA	30	1 LAN Server 1 LAN Switches 1 Desktop 6 Laser Printers 2 Color Printer 4 Multifunctional Devices 1 Workstation per employee	1 fractional T3 (12Mbs)
Phoenix, AZ	9	1 LAN Server 1 LAN Switches 1 Color Printer 2 Multifunctional Devices 1 Workstation per employee	1 T1

Location Name	# of HUD OIG Employees	Infrastructure Hardware Specifics	WAN/LAN Telecommunication Specifics
Pittsburgh, PA	9	1 LAN Server 1 LAN Switches 1 Laser Printer 2 Multifuntional Devices 1 Workstation per employee	1 T1
Potomac Center	26	1 LAN Server 1 LAN Switches 1 Laser Printer 1 Color Printer 3 Multifunctional Devices 1 Workstation per employee	1 T3 (12Mbs)
Richmond, VA	8	1 LAN Server 1 LAN Switches 1 Desktop 1 Laser Printer 1 Workstation per employee	1 T1
Sacramento, CA	5	1 LAN Server (Note 5) 1 LAN Switches 1 Laser Printer 1 Multifunctional Printer 1 Workstation per employee	1 T1
Salt Lake City, UT	2	1 LAN Server (Note 1) 1 LAN Switch 1 Laser Printer 1 Workstation per employee	1 T1
San Antonio, TX	8	1 LAN Server (Note 1) 1 LAN Switch 2 Laser Printer 1 Multifunctional Device 1 Workstation per employee	1 T1

Location Name	# of HUD OIG Employees	Infrastructure Hardware Specifics	WAN/LAN Telecommunication Specifics
San Francisco, CA	11	1 LAN Server (Note 1) 1 LAN Switch 4 Laser Printers 2 Color Printers 2 Multifunctional Devices 1 Workstation per employee	2 T1
Seattle, WA	20	1 LAN Server 1 LAN Switch 5 Laser Printers 2 Color Printers 4 Multifunctional Devices 1 Workstation per employee	2 T1
St. Louis, MO	13	1 LAN Server 1 LAN Switch 2 Laser Printers 1 Multifunctional Deivce 1 Workstation per employee	1 T1
Tampa, FL	13	1 LAN Server 1 LAN Switch 2 Multifunctional Devices 1 Workstation per employee	1 T1
Washington Field Office, DC (Portals)	38	3LAN Server 3 LAN Switches 1 Server 4 Laser Printers 4 Color Printers 1 Multifunctional Device 1 Workstation per employee	1 T3 1 T1
DOJ NCIC		NA	1 T1
CSF		31 Servers 7 Servers 13 Servers 36 Servers	2 T3

Location Name	# of HUD OIG Employees	Infrastructure Hardware Specifics	WAN/LAN Telecommunication Specifics
DRF		20 Servers 2 Servers	2 T3

4.5. DCE HARDWARE AND SOFTWARE

As described in the previous sections, office and user hardware in each office consists primarily of end-user workstations, servers, laser printers, color printers, document management centers, and a limited number of desktops. Specifications of the existing DCE office and user hardware are listed below in Table 6.

Table 6 - Office and User Hardware

Equipment Type	Description	General Specifications (See note)
CSF and DRF Enterprise Servers	These are the servers that run the majority of the applications in the CSF and DRF.	Hardware: Dell 1650 Dell 1750 Dell 2500 Specs: RAM 1.0-3.0 GB Intel 2Ghz – 3GHz Software: OS Windows 2003 Multiple applications
Web Servers	The server for the HUD OIG ISD Intranet.	Hardware: Sun Enterprise 250 Specs: RAM 2GB 4 36GB hard drives Sun OS 5.9 300 Mhz SPARC II Software: Apache Web Server 2.0
Tape Library Servers	Servers for back-up tapes.	ADIC SCALAR 24 / Back up Drive
HUD OIG ISD Office Servers	Each managed office has a LAN server for connection to the WAN.	Hardware: Dell 1650 Compaq 314194-002 Specs: RAM 512MB CPU Intel 1.2 Ghz Software: Windows 2000 SAV, SUS

Equipment Type	Description	General Specifications (See note)
Office Laser Printers	Laser printers located at each office.	Model: HP 2300N HP 2600 HP 3600 N HP 4700
End-User Workstation	Employees currently use laptop computers as their primary computing equipment. Workstation includes a docking station, mouse, keyboard, and flat screen monitor(s).	Hardware: Dell D620, D630, M6300, E6400, M6400 Processor Intel Core Duo 1.6GHz or higher, 80GB or higher hard drive 2 GB or higher RAM Optical Mouse Multimedia Keyboard 9 cell Battery 19" Flat screen LCD Docking station Corporate Back Pack Air/Car/Home/Office Power Cord Software: see Table 7 below

Note: Currently, there may be a mix of equipment types; this table gives the specifics of the primary types of equipment.

Table 7 - Refresh – Laptop Software List

Category	Software
OS	Windows XP (with SP3) – intend to move to Windows 7
Office	Office 2007 (Word, Excel, PowerPoint, Access, Publisher) with SP2 and built-in PDF support– intend to move to Office 2010 .NET Framework with SP1
Mail Client	Microsoft Outlook 2007 and migrating to 2010
Operations Software	AutoAudit
	AutoInvestigation (being phased out; archives maintained)
	Adobe Acrobat 9.0
	ACL v9.1 (not part of base image) – installed on 265 special laptops due to licensing issues
	Citrix 12
Internet Browser	Internet Explorer 7
Anti-Virus Software	Trend Micro
Anti-Spyware Software	Trend Micro
CD Burning Software	Nero 8 (works with Credant –encrypt CD/DVD
Media Software	Real Player 6
	CyberLink Power DVD7 – hardware based

Category	Software
	Windows Media Player 11- hardware based
	QuickTime 7 (but not iTunes) – hardware based
	Flash Player 10 – browser based
	Java.6. - browser based
	Shockwave – browser based
Data Compression Software	Winzip 11
SQL Client	Sybase 12 (install with ACL for auditors)
VPN Client	Verizon IP VPN Client
	Verizon Wireless Boardband Card – Airband 5750 and USB 770
Remote Client Software	LANDesk 8.82
Encryption Software	Credant 6.7
Conference Software Client	Microsoft Office Communications Server (OCS)
Spyware Cleanup	Malwarebytes
Adware Cleanup	Malwarebytes

4.6. SECURITY

HUD OIG ISD security policies and procedures are in place to protect areas where information is vulnerable to intrusion, damage or compromise. Technical security controls are in place to provide identification, authentication, access control, and audit trails. The effectiveness of the security policies and controls has been tested through third-party penetration testing, and security test and evaluation of HUD OIG ISD sites. An annual security assessment is performed, and periodic reviews are executed to ensure that DCE components are compliant with Federal rules and regulations concerning security policies, practices, and processes.

Continuous intrusion detection, malware scanning and inoculating/sanitizing occurs at both the server and user levels. In keeping with NIST directives and good engineering practices, the HUD OIG ISD builds security into the DCE by placing security-related requirements in the network infrastructure, hardware, software, personal, and physical environment requirements tables. The balance of the security-related requirements are found in the requirements for systems/information, personnel, and physical security.

4.7. WEB ENVIRONMENT

HUD OIG ISD currently has an external web presence, and an internal intranet. The infrastructure for the external web presence and the infrastructure for the internal intranet are maintained by the existing contractor. The Contractor shall maintain the infrastructure for both environments. HUD OIG staff is responsible for developing and updating the website content.

4.8. CUSTOM-BUILT APPLICATIONS

HUD OIG ISD has developed a number of custom-built and customized COTS applications to improve its workflow and reporting process. The Contracator shall support the following current customized COTS and custom built applications (described below):

- AutoInvestigation
- AutoAudit
- Case Management Information Sub System (CMISS)
- Employee Database Sub System (EDSS)
- Hot Line Information Sub System (HISS)
- SharePoint

4.8.1. AUTOAUDIT (AA)

AutoAudit is a Lotus Notes based enterprise software application built by Paisley Consulting. This application resides on servers in the CSF, and is accessible by HUD OIG Auditors to enable them to fulfill their mission The CSF provides online storage for over 150 active audit cases and over 1,100 investigative cases in a controlled, secure environment, and 100 GB data storage allows a full five years of case data. HUD OIG ISD has plans to migrate AutoAudit to a new platform.

4.8.2. AUTOINVESTIGATION (AI)

AutoInvestigation is a Lotus Notes based enterprise software application built by Paisley Consulting. This application resides on servers in the CSF, and is accessible by HUD OIG Investigators to enable them to fulfill their mission. Use of AutoInvestigate has been suspended except to close out existing cases and for archive purposes.

4.8.3. SHAREPOINT (SP)

HUD OIG ISD has implemented Microsoft SharePoint 2007 to facilitate collaboration within and among the programs that comprise the agency. SharePoint allows staff to find, share, and author documents using MS Office, use group calendars, post and retrieve announcements, and perform ad-hoc tracking of their day to day work activities. The HUD OIG ISD SharePoint system is segmented such that each division and region is able to maintain its own collaboration site. A Data Steward within each division and region is assigned ownership of their team's site and has administrative rights over the site but not over the server. Additionally, there is a desire to reflect data from other systems (e.g., Investigations, HR databases) on SharePoint. HUD OIG ISD expects the Contractor to support the numerous sub-systems (e.g., Databases, Servers, Network) that comprise the SharePoint platform and to provide a resource capable of performing development when customizations and enhancements are required.

4.8.4. OTHER APPLICATIONS

4.8.4.1 CASE MANAGEMENT INFORMATION SUBSYSTEM (CMISS)

CMISS is a C#.NET based online application that provides the systems support required by the U.S. Department of Housing and Urban Development (HUD) Office of Investor General (OIG) for case management. CMISS enables HUD OIG Investigations and Audits personnel to electronically submit and access essential case information via their web browser, and manage cases from inception to closing via a centralized data repository of case information. This provides a method for remote HUD OIG users and traveling employees to access the CMISS regardless of whether or not they are located within a HUD OIG office.

Special Agents in Charge (SAC), Assistant Special Agents in Charge (ASAC), Supervisory Forensic Auditors (SFA), Forensic Auditors (FA), Special Agents (SA), and support staff document all steps in their assigned investigative activities. Additionally, due to judicial involvement in some of the cases, the files kept and maintained by HUD OIG may be made available to the courts under Discovery.

CMISS and its environment is a secure system where access to information is controlled via a formal process of checks and authorizations involving a hierarchical supervisory structure. CMISS supports the Office of the HUD OIG requirement to maintain a detailed audit trail of cases to closure. This fulfills the requirement to develop a system capable of capturing and maintaining data integrity during the complete case cycle while ensuring data privacy and confidentiality.

4.8.4.2. EMPLOYEE DATABASE SUBSYSTEM (EDSS)

EDSS is a C#.NET based online application that provides the systems support required by HUD OIG for the employee database. It introduces an intranet-based approach which enables OIG personnel to electronically submit and access essential employee information via their Microsoft Internet Explorer web browser. The system provides employee data to CMISS, Hotline Information Subsystem and any other scalable Office of Management and Policy (OMAP) subsystems.

The EDSS application and Employee Database environment is in one central location designated by the HUD OIG Chief Information Office. This ensures data continuity and integrity for all authorized HUD OIG employees. Its centralized data environment is a secure environment where access to information is strictly controlled ensuring data privacy and confidentiality. EDSS supports the Office of the HUD OIG requirement to maintain a detailed repository of employee information.

4.8.4.3. HOTLINE INFORMATION SUBSYSTEM (HISS)

The HISS application provides the Program Integrity Division (PID) with a web-enabled system used to manage “contacts” from their inception to closing via a centralized data repository. A contact contains complainant and subject information and has the capability to expand and include case information when applicable. The Hotline application is the primary report intake operation for HUD's Office of Inspector General (OIG). The Hotline takes reports of fraud, waste, abuse, or serious mismanagement in HUD or HUD-funded programs from HUD employees, contractors, and the public.

4.9. HELP DESK AND SUPPORT

All of the HUD OIG users are currently supported by a Help Desk for any issues they have with their hardware, software or the custom-applications. Through the use of a toll-free number, HUD OIG staff are able to access Help Desk support staff, who are available weekdays 7AM-7PM EST excluding Federal holidays. Support requests can be submitted by email, WEB-based ticket submission, or by leaving a voice message 24x7x365. The Help Desk is the focal point for all seat management services and is staffed to meet agreed-upon service levels. The Help Desk serves as the initial point-of-contact for the customer and is responsible for tracking all trouble tickets,

monitoring each ticket as it moves to resolution, and ensuring the ticket is escalated to the appropriate personnel as necessary. The Help Desk shall be located at the HUD OIG ISD facility and will provide both Tier 1 and Tier 2 support services.

4.9.1. HELP DESK DATA

Requests for assistance come to the Help Desk in a number of ways including: a voice call during business hours; a voice message left after business hours; an email to Help Desk; an internet trouble ticket (user initiated); and a technician initiated trouble ticket. Phone calls for assistance may/may not result in the creation of a trouble ticket.

5.0. PERFORMANCE BASED CONTRACT MANAGEMENT

This is a Performance Based Contract. The Government shall inspect and accept all services delivered pursuant to this Contractor in accordance with the Inspection Clauses (See Section E of the Task Order). In addition, the Performance Requirements set forth the minimum requirements for some of the services performed under this Task Order and may contain a range of acceptable performance for some Contract requirements. Failing to meet a Performance Requirement or failing to perform any Contract requirement in conformance with Contract requirements may reduce the amount of fee payable under the Contract (FAR 52.246-5 Inspection of Services – Cost Reimbursement Apr, 1984).

The Performance Requirements are set forth in a Techniccal Performance Index (TIP). The TIP sets specific the specific Peformance Requirements in the following four (4) categories:

- User Support
- Network Infrastructure Support
- Security
- Project Management

6.0. DCE REQUIREMENTS

The HUD OIG ISD developed the requirements found in this section through a review of the existing contract requirements, by an analysis of mandated changes from NIST, OMB and other oversight organizations, and by gathering additional requirements from HUD OIG ISD Managers. All information and requirements contained within this document are requirements that the Contractor shall provide as part of their service.

6.1. TRANSITION

The Contractor shall transition the existing DCE infrastructure and services from the incumbent contractor. The transition related requirements are presented below in Table 8.

Table 8 - Transition Requirements

Req. #	Description
8-1	The Contractor shall transition the current DCE contractor support from the incumbent to the Contractor. The transition shall take place according to the Transition Plan proposed by the Contractor in its Technical Proposal submitted pursuant to the Solicitation from which this Contract arises. The Transition Plan may be amended as agreed between the Contractor and the Contracting Officer.
8-2	The Contractor shall perform due diligence in preparing for the transition. A due diligence analysis shall consist of two parts: 1) Identification, and 2) Reconciliation. During Identification, the Contractor shall perform a discovery analysis of the existing DCE infrastructure and operation. During Reconciliation, the Contractor may suggest revising the technical solution submitted as part of its Technical Proposal, and recommend the revisions to the Government via the Contracting Officer within thirty (30) days of Contract Award.
8-3	The Contractor shall transition: 1) responsibility for the DCE operation, 2) all government-owned/Contractor purchased DCE infrastructure/equipment, 3) all government-owned/Contractor purchased software, 4) transition of user support from the existing contractor, 5) receipt of all archived and current data, 6) receipt of pertinent documentation, 7) continuity of operations during transition, and 8) security services.
8-4	The Government will provide existing SDLC documentation for the current systems (e.g., CMISS, EDSS, and HISS) to the Contractor during the transition period.

6.2. DCE INFRASTRUCTURE

6.2.1. CENTRAL SERVER FACILITY (CSF) AND DISASTER RECOVERY FACILITY (DRF)

The Contractor shall support and manage the equipment at both the primary facility and back-up facility. This redundancy is critical for continuity of operations. The requirements related to the CSF and the DRF are presented below in Table 9.

Table 9 - CSF and DRF Requirements

Req. #	Description
9-1	The Contractor shall manage the existing equipment at the CSF and DRF where the network and DCE infrastructure for the DCE are located. The DRF shall be able to perform the exact connectivity functions, for HUD OIG ISD identified critical services, of the CSF in the event of a CSF failure.
9-2	The Contractor shall ensure that the DRF has the same connectivity capabilities as the CSF.

9-1	The Contractor shall ensure the CSF will automatically failover to the DRF in support of disaster and COOP instances.

6.2.2. NETWORK INFRASTRUCTURE

The DCE network is comprised of the LANs, VPN and circuits. The network infrastructure requirements are presented below in Table 10.

Table 10 - Network Infrastructure Requirements

Req. #	Description
10-1	The Contractor shall provide operational and maintenance support to the WAN that connects all HUD OIG offices to the CSF and the DRF.
10-2	The Contractor shall provide operational and maintenance support to the baseline network infrastructure for both the CSF and DRF environments.
10-3	The Contractor shall support and maintain the existing local office LAN, and wiring infrastructure
10-4	The Contractor shall design and deploy as required to any new local office(s) LAN, and wiring infrastructure.
10-5	The Contractor shall ensure that it monitors and optimizes network bandwidth and system capacity for the DCE based on all infrastructure and application requirements in this RFP.
10-6	The Contractor shall ensure that any DCE connections to the Internet, or other external networks or information systems, occur through boundary protection interfaces (e.g., web filtering, proxies, gateways, routers, firewalls, encrypted tunnels). The operational failure of the boundary protection mechanisms should not result in any unauthorized release of information outside of the information system boundary.
10-7	The DCE network shall employ information flow control policies and enforcement mechanisms in accordance with NIST and other federal regulations that control the flow of information between designated sources and destinations (e.g., individuals, devices) based on the characteristics of the information.
10-8	The Contractor shall support and monitor nationwide high-speed and other access to the DCE and its components.
10-9	The Contractor shall provide comparable network response times, as specified in the SLA, at all nationwide locations.
10-10	The DCE network shall establish secure communications at new, renovated, or relocated OIG offices in any city in the country.
10-11	The Contractor shall remove all equipment including computer and communications from OIG offices that are closed.
10-12	The DCE network shall allow dial-up access to the network via VPN in addition to high-speed (DSL and cable).
10-13	The Contractor shall allow access to the network from remote locations, this includes mobile user and wireless access to the network.

Req. #	Description
10-14	The Contractor shall not allow any access to the network from remote locations unless the connection is through the VPN.
10-15	The DCE network shall provide the ability to capture the contents of laptop hard drives attached to the network.
10-16	The DCE network only shall support access to email and the internet from HUD OIG ISD issued hand-held devices.
10-17	The DCE network shall not push email to personal Smartphones that are not HUD OIG ISD issued.
10-18	The DCE network shall support application access to all domains and subnets.
10-19	The Contractor shall ensure that, at a minimum, passive scans are executed whenever any hardware (e.g., external hard drive) is connected to the network.
10-20	The Contractor shall provide and manage secure connectivity to the external Web/Internet.
10-21	The DCE network shall provide connectivity to external entities (e.g., Bureau of Public Debt, National Finance Center, local police departments, Department of Justice, and the FBI).
10-22	The Contractor shall support the HUD OIG ISD in securing Interconnection Security Agreements (ISAs) as needed for connectivity with all external entities.
10-23	The DCE network shall ensure connectivity to and compatibility with the HUD network, although the DCE shall maintain a separate and secure network.
10-24	The DCE network shall provide connectivity to the HUD intranet, program applications and internal data sources (e.g., CFO, HR, program offices).
10-25	The DCE network shall provide connectivity to the HUD email directory.
10-26	The DCE network shall provide the ability for authorized users located in one office to share, print and store documents in another office.
10-27	The DCE network shall provide the capability for remote distribution and inventory of software (i.e., software “push”).
10-28	The DCE network shall provide the capability for remote administration of workstations.
10-29	The DCE network shall terminate a network connection at the end of a session, or after a government defined time period.
10-30	The Contractor shall ensure all encrypted communication within the DCE.
10-31	The DCE network system shall establish a trusted communications path between the user and the security functionality of the system.
10-32	The DCE network shall provide the capability to access archived data.
10-33	The Contractor shall deny DCE access to rogue devices.
10-34	The Contractor shall deny access to the DCE from all unauthorized connections or a subversion of authorized connections.
10-35	The Contractor shall support adaptation of IPv6 including integration, testing, and implementation.
10-36	If implemented, the Contractor shall allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access (OMB 06-16).

Req. #	Description
10-37	The Contractor shall satisfy all OMB 06-16 (Reporting Incidents Involving Personally Identifiable Information) requirements except those that are the responsibility of the Government.
10-38	The Contractor shall use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity (OMB 06-16).
10-39	The Contractor shall identify and provide to the HUD OIG ISD all external connections (OMB M-08).
10-40	The Contractor shall insure that all external access points, including internet connections, have been consolidated (OMB 11/2007).
10-41	The Contractor shall insure that all external connections are routed through an OMB-approved Trusted Internet Connection (OMB 11/2007).
10-42	The Contractor shall document, monitor, and control all methods of remote access to the DCE in accordance with government regulations and applicable NIST standards.
10-43	The Contractor shall continuously scan the DCE for vulnerabilities, and malicious code. The Contractor shall propose and present for government approval the selection criteria for 24x7 continuous monitoring.
10-44	The Contractor shall support the HUD OIG ISD implementation of HSPD-12, a presidential mandate for all government agencies that stipulates how all government furnished computers shall be accessed by agency employees. Under this mandate the employee is required to insert their ID badge into a smart card reader on the device and enter their unique 'PIN' number for authentication. HUD OIG ISD is moving forward under this mandate using a phased approach to align the hardware, software, and certificate services necessary for a successful implementation.
10-45	The Contractor shall insure conformance with the requirements of FDCC.
10-46	Contractor shall insure that controls specified for a Moderate Level system as specified by NIST 800-53 Appendix D are instituted and maintained.
10-47	The Contractor shall insure that best practices identified by NIST 800-41 rev 1 are instituted and maintained for firewalls
10-48	The Contractor shall insure that best practices identified by NIST 800-123 are instituted and maintained for general server security.

6.2.3. NETWORK ADMINISTRATION

Continuous network monitoring 24/7 is crucial for ensuring that the DCE is always available to HUD OIG employees, and that the network is operating at the desired performance and availability levels. The network administration requirements are presented in accordance with federal mandates and requirements listed below in Table 11.

Table 11 - Network Administration Requirements

Req. #	Description
11-1	The Contractor shall provide the HUD OIG ISD oversight/monitoring (read access) to the network, servers, and performance tools. This oversight shall be without limit or restriction.
11-2	The Contractor shall implement all tasks required by the contractual obligations. Tasks performed that are outside of the scope of the contractual obligations shall be approved in writing by the Contracting Officer prior to implementation.
11-3	The Contractor shall ensure that any problem causing more than a 99.9% deviation from the target shall be fixed within 1 hour period of time
11-4	The Contractor shall provide real time/near real time network monitoring and network performance tools for monitoring the status and performance of the WAN, the LANs and the DCE. The Contractor shall use these tools to optimize performance of the network.
11-5	The Contractor shall provide 7-days a week and 24-hours a day technical support for the network, in the event of a network related problem. The Contractor must provide support M-F during normal business hours with rapid response capabilities during non-business days/hours.
11-6	The Contractor shall provide onsite support for management of DCE equipment. This will minimally include the following: 1) Developing and planning alternate server and/or user group configurations to meet the needs of classes of users, 2) Creating and maintaining installation disks for easy re-configuration of servers, 3) Maintaining documentation and records of each server configuration, 4) Providing instruction sheets as appropriate for technical staff or computer operators, 5) Documenting software package and operating systems upgrades, patches, and potential replacement software, 6) Upgrading server configurations as needed, 7) Upgrading virus software on the servers as needed, 8) Maintaining software agents on all appropriate servers for configuration information management, 9) Maintaining log/registry of all configuration changes.
11-7	The Contractor shall recommend to the HUD OIG ISD the type and extent of server resources required for the successful implementation of any new LAN application, in keeping with technology advances or emerging industry standards.
11-8	The Contractor shall manage system user/group accounts, which includes but is not limited to establishing, activating, modifying, reviewing, disabling, and removing accounts; specifying access rights/privileges, and identifying account types (i.e., individual, group, and system).
11-9	The Contractor shall ensure that all new account requests are approved in accordance with the MAC Add process.
11-10	The Contractor shall monitor and report the use of specialized user accounts, and remove, disable, or otherwise secure, unnecessary accounts.
11-11	The Contractor shall ensure that HUD OIG ISD managers are notified when information system users are terminated, updated or transferred, and associated accounts are removed, disabled, or otherwise secured in accordance with the MAC Delete process.

6.2.4. WEB INFRASTRUCTURE

The web infrastructure will consist of both external Internet websites, and secure Intranet sites. The web infrastructure requirements are presented below in Table 12.

Table 12 - Web Infrastructure Requirements

Req. #	Description
12-1	The Contractor shall manage and support the HUD OIG ISD web infrastructure. The web infrastructure shall include both the HUD OIG ISD Internet site, and the HUD OIG ISD intranet.
12-2	The Contractor shall monitor the bandwidth and provide resources to support user access to both the HUD OIG ISD Internet and Intranet web sites without degradation.

6.2.5. CUSTOM APPLICATION INFRASTRUCTURE

As described earlier, HUD OIG ISD has five main custom applications:

- AutoAudit (AA)
- AutoInvestigation (AI)
- Case Management Information Subsystem (CMISS)
- Hotline Information Subsystem (HISS)
- Employee Database Subsystem (EDSS)

The Contractor will support these custom applications from an infrastructure perspective. The custom application requirements are presented below in Table 13.

Table 13 - HUD OIG ISD Custom Application Requirements

Req. #	Description
13-1	The Contractor shall ensure existing custom HUD OIG ISD applications are accessible on the DCE network. Additional applications may be developed and will need to be supported under this requirement.
13-2	The Contractor shall work with the development contractor to ensure that all open cases and audits are accessible on-line.
13-3	The Contractor shall work with the development contractor to ensure that all closed cases and audits are archived, but available for searching.
13-4	The Contractor shall work with the development contractor to ensure that there is an accessible index of all archived cases and audits.
13-5	The Contractor shall be responsible for all backup/restore and all backup/restore shall be accomplished in keeping with a documented schedule that is HUD OIG ISD approved.

6.2.6. HARDWARE AND SOFTWARE

6.2.6.1. HARDWARE

DCE Hardware consists of CSF, DRF, and HUD OIG ISD office and user hardware. The Contractor will be responsible for the procurement, as requested by HUD OIG ISD, and support of this hardware. The hardware requirements are presented below in Table 14.

Table 14 - Hardware Requirements

Req. #	Description
14-1	The Contractor shall be proactive in identifying and recommending hardware solutions for optimizing the HUD OIG ISD Enterprise Architecture.
14-2	The Contractor shall ensure that provided hardware meets or exceeds the HUD OIG ISD's needs and capacity requirements for the foreseeable future.
14-3	The Contractor shall procure and deploy to all HUD OIG employees (approximately 750) with lightweight laptop computers. All laptops shall include a docking station, qwerty keyboard, mouse device, and monitor. The laptops should have the capability for quick-release from the docking station, and have a carrying case will all of the necessary equipment to travel with the laptop. This may include power brick, mouse, and other devices as needed.
14-4	The Contractor may be required to procure and deploy combination printer/fax/scanner equipment for selected offices.
14-5	The Contractor shall, based on technical analysis, provide to HUD OIG ISD recommendations and implementation plans related to the selection, deployment and implementation of new hardware to support new applications.
14-6	The Contractor shall develop and maintain on a quarterly basis a Peripheral Catalog listing hardware that HUD OIG staff can select when needed, and the Contractor shall be fully responsible for the interoperability within the DCE of all hardware provided through the catalog.
14-7	The Contractor shall procure and deploy, at a minimum, the following categories of products in the Peripheral Catalog: 1) Printers: laser, color and black & white, including portables, 2) Monitors, 3) CD Devices, 4) Removable Media Drives, 5) Hard Disk Drives, 6) Scanners, including portables, 7) Sound Kits, 8) Plotters, all sizes, 9) Portable Projection System, 10) PCMCIA Adapters, 11) DVD, 12) RAM, 13) Miscellaneous Accessories: mice, carrying cases, keyboards, surge protector, etc.).
14-8	The Contractor shall determine if DCE and user hardware has the functionality and capacity to support the selected peripheral products from the Peripheral Catalog or software from the COTS Software Catalog. The Contractor shall provide recommendations for upgrading hardware features or replacing hardware with a new platform necessary to support the products from either of the catalogs.
14-9	The Contractor shall be fully responsible for the performance of the existing hardware with the new peripherals or software installed.

Req. #	Description
14-20	The Contractor shall ensure that user workstations/laptops have the capability to lock down configurations (except units used for internal testing, units that do not touch DCE, units used by training department, and other non-imaged units) so that modifications cannot be implemented without going through defined change control processes.
14-21	The Contractor shall perform workstation maintenance (e.g., defragment workstation/laptop disks and clean registries) as requested through the Help Desk.
14-22	The Contractor shall inventory all DCE hardware and software for the HUD OIG ISD
14-23	The Contractor shall ensure that hardware meets Energy Star efficiency requirements, and the Contractor shall enable the Energy Star feature prior to deploying the equipment.

6.2.6.2. SOFTWARE

The Contractor will be responsible for providing and supporting HUD OIG ISD approved software for all DCE hardware. The software requirements are presented below in Table 15.

Table 15 - Software Requirements

Req. #	Description
15-1	The Contractor shall be responsible for providing corrective and adaptive maintenance of all HUD OIG developed software (and databases).
15-2	The Contractor shall follow HUD OIG ISD approved policies and procedures and related procedures as documented in the Contractor's Configuration Management Plan when providing corrective and adaptive maintenance of HUD OIG developed software (and databases).
15-3	The Contractor shall follow current HUD OIG ISD coding and naming standards. If there is a conflict between these and voluntary consensus standards the Contractor shall follow voluntary consensus standards.
15-4	The Contractor shall utilize voluntary consensus standards when providing corrective and adaptive maintenance of all HUD OIG developed software (and databases).
15-5	The Contractor's Division or Group that will be implementing this DCE effort shall be currently certified by an external auditor at a CMMI Level 2 or better.
15-6	The Contractor shall deploy and maintain all of the HUD OIG ISD authorized COTS software for the life of this contract.
15-7	The Contractor shall develop and maintain a HUD OIG ISD approved COTS Software Catalog. The catalog shall be updated on a quarterly basis, or at the request of HUD OIG ISD. Products included in the catalog will be identified by the version and release number. The Contractor shall be fully responsible for the interoperability within the DCE of all software provided through the catalog.

Req. #	Description
15-8	The Contractor shall interface with third party vendors on behalf of the HUD OIG ISD and shall supply subject matter expertise (SME) to support the Software Catalog as requested by HUD OIG ISD.
15-9	The Contractor shall, upon the written direction of the HUD OIG ISD, procure and deploy any server or laptop software that is required.
15-10	The Contractor shall, at the direction of the HUD OIG ISD, provide data encryption software that conforms to NIST SP 800-57 and SP 800-13 on the laptops of all end users.
15-11	The Contractor shall deploy new software versions of standard COTS software no earlier than six months after the new version is made commercially available or sooner as directed by HUD OIG ISD. Prior to six months, the Contractor shall require HUD OIG ISD written approval.
15-12	The Contractor shall not deploy new software that has been identified as being problematic until HUD OIG ISD recognizes that the software has stabilized.
15-13	The Contractor shall comply with software usage (e.g., licensing) restrictions. Software and associated documentation shall be used in accordance with contract agreements and copyright laws.
15-14	The Contractor shall provide to HUD OIG ISD, all COTS licenses for which the HUD OIG ISD has paid.
15-15	In the event that the HUD OIG ISD seeks third party sources for training and COTS software support, the Contractor shall support HUD OIG ISD negotiation of the provisions for training and COTS software support that will ensure the integrity of third party provided services.
15-16	The Contractor shall receive written approval from the HUD OIG ISD prior to contracting with a third party source for the provision of training and other COTS software services.
15-17	The Contractor shall support user adoption of the SharePoint services.

6.2.7. SECURITY

The Contractor shall provide system security in compliance with the Federal Information Security Management Act (FISMA), security-related OMB Circulars and Memorandums (e.g., OMB Circular A-130), security-related compliance standards and requirements for federal agencies issued by the National Institute of Standards and Technology (NIST), and any future statutes, regulations, requirements, or guidelines for securing federal systems. Security requirements have been listed in three categories: 1) Personnel Security, 2) Physical Security, and 3) Systems and Information Security.

6.2.7.1. PERSONNEL SECURITY

The Contractor must have the necessary procedures in place to ensure that all personnel working on the project are properly screened and cleared to work on the project. The personnel security requirements are presented below in Table 16.

Table 16 - Personnel Security Requirements

Req. #	Description
16-1	The Contractor shall ensure that all their personnel are U.S. citizens and have a full background investigation for a security clearance (required level will be determined by the HUD OIG ISD) prior to either directly or remotely accessing the HUD OIG ISD computer system(s). HUD OIG ISD has final determination on acceptability. Favorable adjudication is required prior to any access to HUD OIG ISD systems.
16-2	The Contractor shall ensure that any maintenance and operations personnel needing to access DCE data shall have the same clearance level as all Contractor staff on the contract.
16-3	The Contractor shall ensure that personnel and third-party resources it uses for non data related maintenance and dispatch/repairs are escorted and monitored when working in secure areas. The Contractor shall be responsible for any actions of personnel performing activities on their behalf.
16-4	The Contractor shall ensure that all Contractor personnel working on the project take and pass the Basic Systems Security Awareness course approved by HUD OIG ISD, and available on-line before commencing their HUD OIG ISD duties and annually thereafter.
16-5	The Contractor shall have and implement a documented formal sanctions process for personnel failing to comply with established security policies and procedures.
16-6	The Contractor shall ensure that terminated employees have no access to government computing systems immediately prior to their termination in accordance with the MAC Delete procedures.
16-7	The Contractor shall ensure the return of all government information system-related property (e.g., documentation, software, equipment, keys, identification cards, building passes) when an employee is terminated. These shall be surrendered to the HUD OIG ISD immediately upon termination.
16-8	The Contractor shall train personnel in their incident response roles and responsibilities with respect to the DCE, and provide refresher training no less than every twelve (12) months.

6.2.7.2. PHYSICAL SECURITY

The Contractor shall ensure that all facilities, where HUD OIG ISD data and equipment are located, are properly secured to prevent unauthorized access and contact with this data and equipment. The physical security requirements are presented below in Table 17.

Table 17 - Physical Security Requirements

Req. #	Description
17-1	The Contractor shall control all physical access points (including designated entry/exit points) to the HUD OIG ISD computing facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible).

Req. #	Description
17-2	The Contractor shall complete appropriate access agreements (based on approved background checks) for individuals requiring access to the DCE facilities.
17-3	The Contractor shall limit access to the DCE facilities to authorized personnel at all times. The Contractor personnel or agents thereof must present official identification for physical access to equipment.
17-4	The Contractor must establish and maintain a list of personnel with authorized access to DCE facilities. This list must be provided to the government as needed.
17-5	After receiving HUD OIG ISD approval, Contractor personnel shall properly display issued credentials (e.g., badges, identification cards, smart cards) for use within DCE facilities.
17-6	The Contractor shall monitor physical access to DCE information systems to detect and respond to incidents.
17-7	The Contractor shall control DCE information system-related items (i.e., hardware, software) entering and exiting the facility, and maintain appropriate records log of those items.
17-8	The Contractor shall escort all non-cleared personnel performing work functions in the DCE facilities.
17-9	Access to facilities housing storage media shall be strictly controlled with all access recorded in a log.
17-10	Contractor personnel shall not remove equipment or media from the DCE facility until authorized by HUD OIG ISD.

6.2.7.3. SYSTEMS AND INFORMATION SECURITY

At all points throughout the DCE, security must be in place to protect access to systems and the data contained on the systems. The systems and data security requirements are presented below in Table 18.

Table 18 - Systems and Information Security Requirements

Req. #	Description
18-1	The Contractor shall receive Authority to Operate (ATO) security approval from HUD OIG ISD's Designated Approving Authority (DAA) at the conclusion of the transition period.
18-2	The Contractor shall resolve any security findings generated during HUD OIG ISD's security certification and accreditation of the DCE network system, in compliance with federal regulations and implementing NIST standards.
18-3	The Contractor shall detect, prevent, and take action against malicious software (malware) using accepted best practices. This solution shall be maintained and kept current at all times.
18-4	The Contractor shall ensure critical updates, patch management, and system integrity checks, commensurate with the security risk, are tested and implemented.

Req. #	Description
18-5	The Contractor shall provide a security monitoring capability for the HUD OIG ISD Security Manager, with "Read" access to all security monitoring tools and logs.
18-6	The Contractor shall review information system security alerts/advisories (e.g., CERTS, SANS, NIST) as published and take appropriate actions in response.
18-7	The Contractor shall report, in real-time, all computer system and network incidents and attacks to the HUD OIG ISD Incident Response Team.
18-8	The Contractor shall notify the United States Computer Emergency Response Team of all computer system and network incidents and attacks in accordance with the CERT requirements.
18-9	The Contractor shall identify information systems containing proprietary or open source software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). This information shall be reported to the HUD OIG ISD immediately.
18-10	The Contractor shall test and install newly released relevant security patches, service packs, and hot fixes in accordance with federal regulations and the implementing NIST standards.
18-11	The Contractor shall address immediately flaws discovered during security assessments, continuous monitoring, or incident response activities.
18-12	The Contractor shall test the incident response capability for the DCE at least every twelve (12) months using government approved tests and exercises to determine the Cyber Incident Response Plan effectiveness and document the results, and improve where necessary.
18-13	The Contractor shall conduct a self assessment of the security controls in the DCE at least every twelve (12) months to determine the extent to which the system-related controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the network. Any deficiencies shall be reflected in the POAM and resolved in accordance with federal regulations.
18-14	The Contractor shall create and manage network accounts in accordance with the established MAC procedures, consistent with federal regulations and NIST standards
18-15	The Contractor shall create and manage role based systems and data management in accordance with federal regulations and NIST best practices.
18-16	The Contractor shall use appropriate means to control access to various system resources, including review of security logs for indications of unauthorized or inappropriate use of the systems.
18-17	The Contractor shall enforce a limit of consecutive invalid access attempts by a user during a defined time period, in accordance with federal recommendations or industry best practices.
18-18	The Contractor shall limit the number of concurrent sessions for any user.
18-19	The Contractor shall notify the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.
18-20	The Contractor shall insure that the DCE network shall display a HUD OIG ISD approved, system-use notification message before granting system access.

Req. #	Description
18-21	The Contractor shall develop and manage information system authenticators in accordance with federal regulations and the implementing NIST standards.
18-22	The Contractor shall ensure that only HUD OIG ISD approved and authorized/personnel have access to DCE administrator rights.
18-23	The Contractor shall maintain, review, and provide to HUD OIG ISD audit logs as required.
18-24	The Contractor shall ensure that the DCE network records in the audit logs the Administrator's access.
18-25	The Contractor shall provide an automated tool to monitor the DCE for indications of inappropriate and or unusual activity and shall provide the results immediately to HUD OIG ISD upon discovery of such activity.
18-26	The Contractor shall regularly review/analyze audit logs for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
18-27	The Contractor shall archive and index audit logs for management purposes. The audit logs must be available and provided upon HUD OIG ISD management request.
18-28	The Contractor shall ensure that the information system protects audit information and audit tools from unauthorized access, modification, and deletion.
18-29	The Contractor shall ensure that the information system isolates security functions from non-security functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system shall maintain a separate execution domain (e.g., address space) for each executing process.
18-30	The Contractor shall track and document information system security incidents on an ongoing basis, and shall within one hour of discovery report incident information to the HUD OIG ISD Incident Response Team.
18-31	The Contractor shall prohibit the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information.
18-32	The Contractor shall obtain concurrence from the HUD OIG ISD Federal Security Team prior to implementing any change to network security.
18-33	The Contractor shall ensure that only a Three-key Triple DES Encryption and Decryption be used as described in NIST 800-13.
18-34	The Contractor shall insure that personal information collected for employee and contractor identification purposes is handled consistent with the Privacy Act of 1974 (5 U.S.C. § 552a) and OMB 06-16.
18-35	The Contractor shall encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by the HUD Deputy Secretary or an individual he/she may designate in writing (OMB 06-16).
18-36	The Contractor shall log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required (OMB 06-16).

Req. #	Description
18-37	The Contractor shall insure that to effectively deploy DNSSEC, the Contractor shall follow recommendations in NIST Special Publication 800-81 "Secure Domain Name System (DNS) Deployment Guide." Procedures for assessing DNSSEC controls are described in NIST's Special Publication 800-53A "Guide for Assessing the Security Controls in Federal Information Systems (OMB 08-23).
18-38	The Government will satisfy all the requirements of OMB 09-32 including those requirements for executing essential agreements to facilitate integrating the National Cyber Protection system and for synchronizing with US-CERT.
18-39	The Government will develop and promulgate formal, documented policies governing minimum security requirements as set forth in FIPS 200.
18-40	The Contractor shall insure that all security controls identified for a moderate level system are implemented and supported in the DCE (FIPS 200).
18-41	The Contractor shall insure that all requirements identified in NIST 800-18 rev 1 or newer are satisfied. The Contractor shall not be responsible for satisfying any requirement that belongs to the System Owner.
18-42	The Contractor shall conduct assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. NIST Special Publication 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.

6.3. CONFIGURATION MANAGEMENT

Configuration management is the process of controlling changes to the DCE. These changes include modifications to CSF and DRF hardware, software, network changes and other actions that change the configuration or operating of major DCE components. HUD OIG ISD will have a Configuration Control Board (CCB) that shall review and approve all major configuration changes. The configuration management requirements are presented below in Table 19.

Table 19 - Configuration Management Requirements

Req. #	Description
19-1	The Contractor shall utilize configuration control as documented in the Contractor's HUD OIG ISD approved Configuration Management Plan.
19-2	The Contractor shall track changes to the DCE environment with documented change requests (CRs) and report on the status of the CR's at the monthly CCB meetings.
19-3	The Contractor shall allow HUD OIG ISD access and transparency into the Contractor's automated configuration management tool.
19-4	The Contractor shall archive and index audit logs for any configuration changes to the DCE. The audit logs must be available and provided upon HUD OIG ISD management request.
19-5	The Contractor shall maintain an automated Change Request Log and this shall be available to the HUD OIG ISD upon request.

Req. #	Description
19-6	The Contractor shall maintain an automated Problem Request Log and this shall be available to HUD OIG ISD upon request.
19-7	The Contractor shall insure that best practices identified by Draft NIST 800-128, Appendix F are instituted and maintained for configuration management.

6.4. MOVES, ADDS AND CHANGES

Moves, adds and changes refer primarily to actions related to users and their equipment, e.g., user workstations, user accounts, user location, etc. The move, add and change requirements are presented below in Table 20.

Table 20 - Moves, Adds and Changes Requirements

Req. #	Description
20-1	The Contractor shall develop, for HUD OIG ISD approval, Standard Operating Procedures for MACs. These documented Standard Operating Procedures shall be updated and maintained.
20-2	The Contractor shall utilize and maintain the current HUD OIG ISD mechanism/system used for requesting moves, adds, and changes.
20-3	The Contractor shall coordinate with Government entities, to ensure physical office moves as per the Contractor's HUD OIG ISD approved Standard Operating Procedures are properly executed.

6.5. ASSET MANAGEMENT

Asset management involves keeping an accurate account and inventory of all of the Contractor provided DCE equipment. The requirements for asset management are presented below in Table 21.

Table 21 - Asset Management Requirements

Req. #	Description
21-1	The Contractor shall use an automated means for tracking all of the DCE assets. The software must meet the approval of the HUD OIG ISD, and the Contractor must allow the HUD OIG ISD "Read" access to this database.
21-2	The Contractor shall, within 30 days of contract signing, identify and document its methodology for auditing assets in place and reconciling with inventory identified in the contract.

6.6. TECHNOLOGY REFRESH

To ensure that the HUD OIG is taking advantage of new technologies, and to replace DCE equipment that may be performing at a less than optimal rate due to regular and long-term use, the Contractor shall perform a refresh of DCE equipment as directed by the Government. The technology refresh requirements are presented below in Table 22.

Table 22 - Technology Refresh Requirements

Req. #	Description
22-1	The Contractor shall refresh DCE equipment and software at intervals as prescribed by HUD OIG ISD.
22-2	The Contractor shall prepare, at HUD OIG ISD direction, a refresh proposal outlining the DCE assets to be refreshed, the specifications of the new equipment, and the timing of the refresh.

6.7. OPERATIONS AND MAINTENANCE

To ensure successful and continued operation of the DCE and its components, the Contractor will be responsible for performing operational tasks as well as preventative, corrective, adaptive maintenance and emergency repair of the equipment in the DCE. The operations and maintenance requirements are presented below in Table 23.

Table 23 - Operations and Maintenance Requirements

Req. #	Description
23-1	The Contractor shall schedule, perform, and document routine preventative and regular operations and maintenance on DCE components in accordance with manufacturer or vendor specifications and/or HUD OIG ISD's requirements.
23-2	The Contractor shall be able to support on-site repair and replacement of DCE equipment, at all HUD OIG ISD locations.
23-3	The Contractor shall support ad-hoc operations and maintenance activities for which the Contractor shall "ramp-up" quickly to meet special demands for activities that require immediate response.
23-4	The Contractor shall perform operational infrastructure support in the form of cabling installation and repair, e.g., associated with renovations, as well as the opening of new offices in the future.
23-5	The Contractor shall document, with blueprints, all new and modified cabling associated with renovations, as well as the opening of new offices.
23-6	The Contractor shall not make or cause to be made alterations to Government owned or controlled real property facilities, buildings, structures, components, systems, or utilities during the course of implementing this tasking, either temporarily or permanently, without the permission of the Government.
23-7	The Contractor shall maintain maintenance logs for all remote maintenance, diagnostic, and service activities.
23-8	The Contractor shall approve, control, and monitor remotely executed maintenance and diagnostic activities.
23-9	The Contractor shall approve, control, and monitor the use of information system maintenance tools and maintain the tools on an ongoing basis.
23-10	The Contractor shall terminate all sessions and remote connections when remote maintenance is completed.

Req. #	Description
23-11	If password-based authentication is used during remote maintenance, the Contractor shall change the passwords following each remote maintenance service. Other techniques to consider for improving the security of remote maintenance include: 1) encryption and decryption of diagnostic communications; 2) strong identification and authentication techniques, such as tokens; and 3) remote disconnect verification.
23-12	The Contractor shall prevent loss of information during all operations and maintenance activities by taking steps to protect and, at the HUD OIG ISD's direction, restore, as necessary, any information residing in the equipment being maintained.
23-13	The Contractor shall obtain maintenance support and spare parts for DCE components to ensure that the maintenance and repair related performance metrics are met.
23-14	The Contractor shall check all maintenance equipment with the capability of retaining information to ensure the equipment is appropriately sanitized before release. If the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.
23-15	The Contractor shall maintain a list of individuals authorized to perform maintenance on the information system and only authorized individuals shall perform maintenance on the systems within the DCE.
23-16	The Contractor shall employ automated mechanisms to ensure only authorized personnel use maintenance tools.
23-17	The Contractor shall supervise maintenance personnel during the performance of maintenance activities on the DCE systems when maintenance personnel do not have the required access authorizations.
23-18	The Contractor shall ensure that prior to removal of any hardware or storage device for repair or replacement, all user data and software have been backed up.
23-19	The Contractor shall insure that all storage media, prior to removing for repair, replacement, recycling, reusing, donating, or disposal, be erased using a repeated overwrite operation, purged, degausessed or destroyed in accordance with FISCAM section AC 3.4, NIST SP 800-18, NIST SP 800-26 and the NIST System Development Life Cycle Policy.
23-20	The Contractor shall track, document, and verify media sanitization actions and periodically test sanitization equipment/procedures to ensure correct performance.
23-21	The Contractor shall be responsible for notifying the HUD OIG ISD if a hard disk containing information has been inadvertently shipped to a maintenance depot or Contractor site.
23-22	The Contractor shall conduct regular backups (e.g., nightly, weekly) of user-level and system-level information contained in the information system and store backup information at HUD OIG ISD approved secured location. The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) should be consistent with the HUD OIG ISD's recovery time objectives.

Req. #	Description
23-23	The Contractor shall create, after an agreed-upon time designated by HUD OIG ISD, accessible data archives.
23-24	The Contractor shall archive all closed audit and investigation cases from the AI/AA applications, quarterly, on a non-volatile media to prevent manipulations and changes to data.
23-25	The Contractor shall provide a robust audit trail for any date movement to/from the non-volatile media storing closed audit and investigation cases from the AI/AA applications.
23-26	The Contractor shall maintain an index of all archived data that allows for effective and efficient locating of files.
23-27	The Contractor shall affix external labels to removable information storage media indicating the distribution limitations and handling caveats of the information.
23-28	The Contractor shall control information system media (paper and electronic) and restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.
23-29	The Contractor shall physically control and securely store information system media, both paper and electronic, based on the highest FIPS 199 security category of the information recorded on the media.
23-30	The Contractor shall update the current test lab and test any acquired software, software updates, and patches on the HUD OIG ISD configured laptop or server. Only software that has passed Acceptance Testing shall be placed in the DCE.
23-31	The Contractor shall employ the necessary automated tools using remote technology to distribute software to servers and workstations electronically.
23-32	The Contractor shall employ the necessary automated tools provide remote diagnostics and management of workstations and servers.
23-33	The Contractor shall deploy COTS software upgrades/patches as directed by the HUD OIG ISD. The Contractor is responsible for fielding and vetting the findings as soon as they are commercially available. All upgrades/patches must be tested before deployment.
23-34	The Contractor shall insure that all the requirements of NIST 800-40 (latest approved version) are met for patch and vulnerability management.
23-35	The Contractor shall deploy COTS software upgrades/patches only after testing on the HUD OIG ISD configured laptop/server in the official test lab environment.
23-36	In the event that a nonrepairable problem occurs in the Operational environment as a result of an implemented upgrade/patch, the Contractor shall perform a roll-back in accordance with the process described in the HUD OIG ISD approved Patch Procedures.
22-37	The Contractor shall apply patches in accordance with NIST SP 800-40 (latest revision). The Contractor shall use only HUD OIG ISD approved test documentation for acceptance testing of software upgrades/patches. All test documentation shall be based on the most recent version of IEEE Std. 829. Test documentation shall include a test plan, test cases, test procedures, and a test report.

Req. #	Description
22-38	The Contractor shall provide back/up restore services to the SharePoint and related servers including the SQL Server.
23-39	The Contractor shall verify DCE functionality and system security features after changes have been made.
23-40	The Contractor shall satisfy all OMB 07-11 requirements pertaining to the approved FDCC configuration and settings.
23-41	The Contractor shall satisfy all OMB 07-18 requirements pertaining to the operations and maintenance of the approved FDCC configuration and settings.
23-42	The Contractor shall support milestone events including but not limited to periodic operational readiness reviews, scheduled maintenance, and monthly releases.

6.8. OUTAGE PREVENTION AND DISASTER RECOVERY

In the design of its data centers, the Contractor must include elements that safeguard against outages of the DCE. The Contractor must also have plans and facilities in place to ensure continued operations of HUD OIG ISD identified critical functions in the event of a disaster or major damage to the CSF. The outage prevention and disaster recovery requirements are presented below in Table 24.

Table 24 - Outage Prevention and Disaster Recovery Requirements

Req. #	Description
24-1	The Contractor shall, in conjunction with the HUD OIG ISD, prepare a prioritization of functionalities that will be made available after a disaster.
24-2	The Contractor shall document its mechanisms and procedures to ensure the CSF or DRF can be recovered and reconstituted to its original state and can remain operational during a disaster or failure.
24-3	The Contractor, in the event of a disaster or other loss of operation of the CSF, shall ensure that the DRF shall provide continuity of operations until the CSF can be restored to full functionality. Once the CSF is returned to service, the Contractor shall replicate data from the DRF to the CSF to ensure no loss of data to HUD OIG ISD users.
24-4	The Contractor shall test the HUD OIG ISD approved DCE Contingency Plan capability every twelve (12) months using documented exercises to determine the plan's effectiveness.
24-5	The Contractor shall support the development of a HUD OIG ISD approved Continuity of Operations (COOP) Plan in accordance with National Security Presidential Directive (NSPD) 51/Homeland Security Presidential Directive (HSPD) 20, *National Continuity Policy*; the National Continuity Policy Implementation Plan; Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*; and other related Directives and guidance. This plan shall be updated upon request.
24-6	The Contractor shall train personnel in their DCE contingency roles and responsibilities and provide and document refresher training every twelve (12) months.

Req. #	Description
24-7	The Contractor shall provide the capability to shut off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak), without endangering personnel by requiring them to approach the equipment in the DRF.
24-8	The Contractor shall protect DCE power equipment and cabling from damage and destruction in the CSF and DRF.
24-9	The Contractor shall monitor the temperature and humidity within the CSF and DRF to ensure that the levels remain within acceptable parameters.
24-10	The Contractor immediately implement mitigation procedures in the event either temperature or humidity exceed their acceptable parameters. Mitigation procedures shall be vigorously pursued and escalated until such time as environmental conditions are restored to their acceptable operating parameters.
24-11	The Contractor shall report all potential threats to service and integrity of data immediately to the HUD OIG ISD and initiate emergency procedures as identified in the Disaster Recovery Plan.

6.9. USER SUPPORT/ HELP DESK

Providing reliable and knowledgeable assistance to HUD OIG ISD users is a very important component of the support required under this RFP. Because many users are mobile and rely on their laptops to perform their work, easy access and prompt user support is necessary to minimize non-productive time. The user support/help desk requirements are presented below in Table 25.

Table 25 - User Support/Help Desk Requirements

Req. #	Description
25-1	The Contractor shall have a single, integrated help desk that is the central management point for user-reported problems related to the DCE and user hardware. The help desk shall be dedicated, and operate 12 hours a day, 5-days a week, 52 weeks a year excluding all Federal holidays.
25-2	The Contractor shall field all calls pertaining to the DCE, and redirect problems and questions related to custom-built applications and telephone problems to other appropriate help desks or subject matter experts.
25-3	The Contractor shall ensure that the help desk can answer 75.0% of user DCE issues, excluding 'Test', Projects, MACs, XEROX/RICOH, Break/Fix, Maintenance, and Security alerts; and, employ an escalation process involving qualified technical personnel that handle more complex issues.
25-4	The Contractor shall provide the ability to reach the Help Desk via phone, e-mail or on the web. The web shall be used to also check status of submitted tickets.
25-5	The Contractor shall use an automated trouble-ticket management system at the help desk.
25-6	The Contractor shall recommend an automated call data system that will enable automatic routing of the call to the next available staff.

Req. #	Description
25-7	The Contractor shall recommend service desk software that will enable trouble ticket management, reporting, and back office services.
25-8	The Contractor shall provide the HUD OIG ISD on-line access to the trouble ticket system.
25-9	The Contractor shall provide a method by which HUD OIG ISD may directly produce regular and ad hoc reports and statistics from the trouble ticket system.
25-10	The Contractor shall ensure that the help desk has in place documented problem resolution escalation procedures.
25-11	The Contractor shall develop and provide for its help desk staff a help desk manual. The help desk manual should cover an overview of the Contractor's DCE environment and include guidance on assisting HUD OIG customers in all of the areas in which they would call for assistance.
25-12	The Contractor shall identify, by HUD OIG location, the local onsite, local offsite, and remote resource levels and expertise it plans to have. The Contractor shall identify the level and expertise of staffing based on the range of seats supported at each distinct location type (such as large metropolitan area, small metropolitan area). .
25-13	The Contractor shall ensure that all safety rules, regulations, and procedures are followed by the Contractor's staff when at a HUD OIG facility providing user support.
25-14	The Contractor shall ensure that their staff demonstrates professional conduct in accordance with HUD OIG ISD standards.
25-15	The Contractor shall provide user laptop support. If the problem cannot be resolved through the help desk and the laptop must be taken from the user for repair or replacement, the Contractor shall provide a replacement laptop with the standard configuration plus all user-specific data and software. The user shall not experience more than one (1) business day's interrupted usage of, or access to the user's data, email, and the HUD OIG network.
25-16	The Contractor shall ensure, prior to shipment, that laptops that are sent out to users (e.g., during a repair) work properly.
25-17	The Contractor shall notify HUD OIG ISD immediately when system components or applications are experiencing problems.
25-18	The Contractor shall notify users immediately when changes to the network or systems have been made that may affect the users.
25-19	The Contractor shall respond to calls or emails requesting Help Desk assistance within 1 minute and 2 hours respectively. Date and Time of Request shall be recorded and Date and Time of Response shall be recorded. The nature of the resolution shall be recorded.
25-20	The Contractor shall create an automated satisfaction survey that is sent to the user whenever a Trouble Ticket is closed. The results of those surveys shall be included in the monthly report to the HUD OIG ISD.
25-21	The Contractor shall provide Help Desk support that is equivalent to Tier 2 support. Required support that is equivalent to Tier 3 or 4 shall not be provided by the Help Desk but shall be referred to the HUD OIG ISD Subject Matter Expert.

Req. #	Description
25-22	The Contractor shall provide a reporting system that offers standardized and ad hoc queries and reports to the HUD OIG ISD.
25-23	The Contractor shall provide read/execute access of the reporting system to the HUD OIG ISD.
25-24	The Contractor shall provide an on-line trouble ticket system that provides: a unique ID number; a short description of the problem; a long description of the problem; the date/time the ticket was created; the severity/criticality of the problem; a description of the resolution; the date/time of the resolution; the identification of the person(s) fixing the problem; the date/time the resolution passed testing; the identification of the person executing the test(s).
25-25	The Contractor shall provide an on-line trouble ticket system that supports the recording, and tracking of network, software, and hardware problems and resolution.

7.0. PERSONNEL

The Contractor shall staff this project with a team of highly qualified personnel, versed in the areas of project management, infrastructure, system security, system engineering and user support. The personnel requirements are presented below in Table 26.

Table 26 - Personnel Requirements

Req. #	Description
26-1	The Contractor shall provide and maintain a current list of Contractor personnel (e.g., pending, approved, disapproved) designated to work on the contract.
26-2	The Contractor shall provide written notification at least 10 calendar days, when possible, in advance, prior to any personnel reassignment, removal, or resignation. The notification shall be submitted to the Contracting Officer and include justification in sufficient detail to permit evaluation of the impact of the proposed change on the program and its schedule.
26-3	The Contractor shall provide resumes for any personnel replacements, and the Contractor must demonstrate that the qualifications of the prospective replacement personnel are equal to or better than the qualifications of the personnel being replaced.
26-4	The Contractor shall insure that all personnel slots are filled within 30 calendar days. Personnel slots that are vacant for more than 60 days shall result in a penalty unless the delay is not in the control of the Contractor such as a delay in the granting of a security clearance.
26-5	The Contractor shall, remove immediately from the HUD OIG ISD workplace, any of Contractor's staff who, after 120 days probation, HUD OIG ISD determines do not have the requisite skills or knowledge to perform their assignment(s).
26-6	The Contractor shall ensure that no replacements of personnel are made by the Contractor without the concurrence of HUD OIG ISD.

Req. #	Description
26-7	The Contractor shall pay for the cost of security clearances for its personnel.
26-8	The Contractor shall not fill any slot with individuals failing to meet the minimum HUD OIG ISD mandated requirements.
26-9	The Contractor shall provide a Help Desk Manager with experience managing multiple Help Desks of comparable size and complexity. HUD OIG ISD prefers 7 years experience managing Help Desks that included Tier 1 and Tier 2 responsibility.
26-10	The Contractor shall provide a Security Manager with a current CISSP certification. HUD OIG ISD prefers 8 years of relevant experience.
26-11	The Contractor shall provide security support staff with experience in a comparable environment. HUD OIG ISD prefers 6 years of relevant experience.
26-12	HUD OIG ISD prefers the Contractor provide a Project Manager with a PMP and 10 years of relevant experience in a comparable environment.
26-13	HUD OIG ISD prefers the Contractor assign personnel to support DCE with 2 or more years of comparable infrastructure and operations experience.
26-14	HUD OIG ISD prefers the Contractor provide Team Leads with 5 years of comparable infrastructure and operations experience.
26-15	The Contractor shall be responsible for insuring that all personnel have the requisite certifications and that said certifications are current.
26-16	The Contractor shall be responsible for insuring that all Contractor personnel billed to this effort sign and provide to HUD OIG ISD a signed copy of the HUD OIG ISD's rules of behavior no later than close of business of their first day.
26-17	The Contractor shall be responsible for insuring that all Contractor Personnel complete a government furnished security awareness training course and provide a signed Certificate of Completion to HUD OIG ISD no later than close of business of the fifth business day of assignment.

8.0. QUALITY ASSURANCE (QA)

QA processes and procedures are developed and implemented to ensure that high quality service is being provided to the HUD OIG ISD. These processes and procedures are also put into place to provide a means of proactively identifying areas that may need improving. The Contractor shall use a documented quality assurance process in supporting the operations and maintenance of the DCE. The QA process and procedure requirements are presented below in Table 27.

Table 27 – Quality Assurance Requirements

Req. #	Description
27-1	The Contractor shall ensure that its quality assurance includes, but is not limited to: monitoring and managing service level performance; conducting trend analysis; delivering performance reporting to the HUD OIG ISD; having problem resolution procedures in place, and supporting HUD OIG ISD validation of the Contractor's contract performance reporting.

Req. #	Description
27-2	The Contractor shall submit for HUD OIG ISD approval documentation for testing of hardware and software. Test documentation shall include a test plan, test cases, test procedures, and a test report
27-3	The Contractor shall identify and manage risks that may affect the DCE or the proposed management approach in the Contractor's Risk Management Plan.
27-4	The Contractor shall identify its mitigation strategy for any high risks identified in the Contractor's Risk Management Plan.
27-5	The Contractor shall have documented procedures for measuring customer satisfaction and modifying service levels to achieve customer satisfaction objectives specified in the SLA.
27-6	The Contractor shall document and employ its approach for communicating and executing individual task requirements, resolving technical, service, and personnel issues between the Contractor's key personnel and the HUD OIG ISD.
27-7	The Contractor shall participate in ad hoc working groups established by the HUD OIG ISD, as required.
27-8	The Contractor shall support and cooperate with independent verification and validation (IV&V) initiatives, as directed by HUD OIG ISD.
27-9	The Contractor shall respond to all findings, regarding Contractor's deliverables, identified during the IV&V evaluation and found acceptable by HUD OIG ISD.
27-10	The HUD OIG ISD will evaluate all security-related Contractor generated documentation, for acceptance purposes, based on the applicable NIST standard.
27-11	The HUD OIG ISD will evaluate all non-security Contractor generated documentation (e.g., Quality Assurance Plan, Test Documentation), for acceptance purposes, based on the applicable voluntary consensus standard.(ISO, IEEE, ANSI) in lieu of government-unique standards except where inconsistent with law or otherwise impractical (OMB Circular A-119(R).

9.0. DOCUMENTATION

The Contractor shall develop, deliver to HUD OIG ISD for acceptance, and regularly update a prescribed set of DCE-related documentation. The documentation requirements are presented below in Table 28.

Table 28 - Documentation Requirements

Req. #	Description
28-1	Deliverable—The Contractor shall, within 30 days of contract signing, develop and submit for HUD OIG ISD approval an **Operations and Maintenance Plan** that conforms with contract requirements and that documents the Contractor's approach for operating and maintaining the DCE. At a minimum, the **Operations and Maintenance Plan** shall address the following areas: 1) The DCE specifications including but not limited to infrastructure diagrams, configurations and capacity by location, or type of location, 2) Baseline services provided, 3) User support and Help Desk procedures, 4) Staffing coverage for HUD OIG locations, 5) Technology refresh methodology, 6) Service assurance, 7) DCE management team and approach, and 8) Contractor and HUD OIG ISD roles and responsibilities.
28-2	Deliverable—The Contractor shall deliver an updated **Operations and Maintenance Plan** after each revision of the DCE, and at least annually at the beginning of each contract year.
28-3	Deliverable—The Contractor shall, within 10 days of contract signing, develop and submit to HUD OIG ISD for approval a **Transition Plan**. The Transition Plan shall include but not be limited to: infrastructure, communication, operations, databases, hardware, and software. No Transition shall take place until the Government approves the Transition Plan. The **Transition Plan** (TP) shall document how the Contractor will transition the existing environment to the new environment. The TP shall include but is not limited to the following sections: 1) Transition approach, 2) Transition and deployment schedule listing all pertinent activities, 3) Interim service solution approach, 4) Transition staffing, 5) Transition risk mitigation, 6) Organization awareness and communications, 7) Results of DCE Discovery and associated impacts to the transition, and 8) Full operations readiness checklist.
28-4	Deliverable—The Contractor shall, during transition, conduct, document and submit to HUD OIG ISD a **Privacy Impact Assessment** on the systems within the DCE. OMB Memorandum 03-22 provides guidance for conducting a privacy impact assessment (PIA).
28-5	The Contractor shall develop and maintain a current **Baseline Configuration Document** that contains an inventory of the system's components. The inventory of information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture).
28-6	Deliverable—The Contractor shall, within 30 days of contract signing, develop and submit to HUD OIG ISD for approval a **Contingency Plan** based on NIST SP 800-34 (latest version).

Req. #	Description
	The **Contingency Plan** shall document procedures and capabilities for recovering the DCE when a disaster or a break in DCE service occurs. The plan shall detail what steps will be taken to ensure continuity and restoration of services. The Contractor shall review the contingency plan every twelve (12) months and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.
28-7	Deliverable—The Contractor shall, within 30 days of contract signing develop and submit to HUD OIG ISD for approval, a comprehensive **DCE System Security Plan**. The plan, in accordance with NIST SP 800-18 (latest version), should address the following areas of security and policy: Section 1) Information systems and data security; Section 2) Personnel security; Section 3) Facility security; and Section 4) Security Awareness and Training. The plan shall describe the purpose, scope, roles, responsibilities, and compliance with all security related matters. Section 1 should contain, at a minimum, details on: a) user identification and authentication, b) access to systems, including remote access, c) audit trails, d) media protection, e) malware and intrusion tools and techniques, and f) security incident response and reporting, which includes containment, eradication, and recovery. The Contractor shall review the plan every six (6) months and revise it to address system/organizational changes or problems identified during plan implementation or security control assessments.
28-8	Deliverable— The Contractor shall, within 30 days of contract signing, develop and submit to HUD OIG ISD for approval a **Continuity of Operations (COOP) Plan**, based on Federal legislation and directives that detail the procedures and guidance to sustain the HUD OIG ISD mission essential functions at an alternate site for up to 30 days.
28-9	Deliverable—The Contractor shall deliver an updated **Continuity of Operations (COOP) Plan**, and at least annually at the beginning of each contract year.
28-10	Deliverable—The Contractor shall within 30 days of contract signing, develop and submit to HUD OIG ISD for approval a **Cyber Incident Response Plan**, based on NIST 800-14 (latest version), that details how risks to the DCE will be identified and mitigated.
28-11	Deliverable—The Contractor shall deliver an updated **Cyber Incident Response Plan** every twelve (12) months or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.
28-12	Deliverable—The Contractor shall within 30 days of contract signing, develop and submit to HUD OIG ISD for approval a **Risk Management Plan**, based on NIST 800-14 (latest version), that details how risks to the DCE will be identified and mitigated.
28-13	Deliverable—The Contractor shall deliver an updated **Risk Assessment Plan** every twelve (12) months or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the

Req. #	Description
	system.
28-14	Deliverable—The Contractor shall, within 30 days of contract signing, develop and submit to HUD OIG ISD for approval develop, disseminate, and update, at least annually, a **System Maintenance Plan** that details how regular and emergency maintenance to DCE components will be performed.
28-15	Deliverable—The Contractor shall maintain the following documentation: 1) Procedural manuals and standard operating procedures, 2) Current editions of all documentation pertaining to COTS software applications and hardware in use within the DCE, and 3) As required, bulletins, newsletters, web-based information, and other documentation to inform users about Help Desk operations and other related IT support functions pertaining to them.
28-16	Deliverable—The Contractor shall insure that all security-related documentation identified by NIST 800-18 rev 1 (or later version) shall be generated in accordance with that standard.
28-17	Deliverable—The Contractor shall establish and maintain a virtual library that contains, at a minimum, all of the HUD OIG ISD approved required documentation (CDRLs).
28-18	Deliverable—The HUD OIG ISD will provide the Contractor with a **Communications Plan** within 30 days of Contract Signing. This plan will include but not be limited to: Government Points of Contact for the various functional areas (e.g., infrastructure, operations, maintenance, security); reporting infrastructure; and issue resolution.
28-19	Deliverable—The Contractor shall, within 30 days of contract signing, develop and submit to HUD OIG ISD for approval **a Quality Assurance Plan** in accordance with the most recent version of IEEE Std 730.
28-20	Deliverable—The Contractor shall, within 30 days of contract signing, develop and submit to HUD OIG ISD for approval a **Project Management Plan** based on the most recent version of IEEE Std 16326. The PMP shall describe the methodology by which the Contractor intends to manage the various functional areas (e.g., operation/maintenance, security, network administration, and user support) and the anticipated schedule including baseline milestones.
28-21	Deliverable—The Contractor shall generate and deliver to the Government software-related documents that are recommended by the most recent version IEEE Std 1012 for software (both in development or enhancement or fix) that has an integrity level commensurate with MODERATE. Such documents include but are not limited to: Requirements Document, Design Document, Test Plans (integration, system, acceptance), Test Cases and procedures (integration, system, acceptance).
28-22	Deliverable—The Contractor shall, within 30 days of contract signing, develop and submit to HUD OIG ISD for approval **a Sharepoint Backup/Restore Plan** based on NIST SP 800-26.
28-23	Deliverable—The Contractor shall maintain and update all delivered Plans annually or when there are changes to the environment, the infrastructure, the operations or the networks that require a change to the existing process or procedures.

Req. #	Description
28-24	Deliverable—The Contractor shall, within 30 days of contract signing, develop and submit to HUD OIG ISD for approval a **Sharepoint Maintenance Plan**. The Sharepoint Maintenance Plan shall include but not be limited to: code maintenance and updates, configuration of Sharepoint lists, creation of workflows, new Sharepoint databases, and optimizing database architecture and load balancing.
28-25	Deliverable—The Contractor shall provide to the Government, on a periodic basis, updates of process and procedures for maintaining the email and Smartphone systems.
28-26	Deliverable – The Contractor shall, within 30 days of contract signing, develop and submit to HUD OIG ISD for approval a **DCE Configuration Management Plan based on the most recent version of IEEE 828** that includes but is not limited to Configuration Identification, Configuration Control, Configuration Status Accounting, and Configuration Audits.
28-27	Deliverable—The Contractor shall deliver an updated DCE **Configuration Management Plan** every twelve (12) months or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the management of the system.
28-28	Deliverable—The Government will provide a Configuration Management Process and a Risk Management Process within 10 days of contract signing.
28-29	The Contractor shall provide for HUD OIG ISD approval, a solution for sharing unusually large files with authorized users in external agencies.

10.0. MISCELLANEOUS SERVICES

10.1. RESEARCH AND ANALYSES

To ensure that the DCE is taking advantage of the latest technology, the Contractor should proactively conduct research and analyses to identify and recommend improvements or enhancements in technology that would benefit the HUD OIG ISD. The research and analyses requirements are presented below in Table 29.

Table 29 - Research and Analysis Requirements

Req. #	Description
29-1	The Contractor shall proactively perform research and analyze the feasibility of new technology that could be implemented in the DCE. This research and analysis must be approved in advance by the HUD OIG ISD, and result in documented analysis accompanied with recommendations.
29-2	The Contractor shall provide technical and/or business enhancement recommendations to HUD OIG ISD at scheduled technology reviews. Periodic review of these findings shall be reported to the HUD OIG ISD. When directed by HUD OIG, the Contractor shall prepare a white paper to describe technical and business advantages of the recommendations and an estimated cost to implement.

10.2. OPTIONAL SERVICES

The HUD OIG ISD has identified services that are not needed at this time, but may be needed as conditions warrant. When a need for one of these optional services arises, the Contracting Officer will submit the requirements to the Contractor and the Contractor will analyze the requirements and submit to the Contracting Officer and Technical Proposal and a Cost Proposal for implementation of the services. An example of these optional services requirements is presented below in Table 30.

Table 30 - Optional Requirements

Req. #	Description
30-1.	The Contractor shall provide the means of developing software applications for the HUD OIG ISD (e.g., a HUD OIG ISD management information system).

11.0. REPORTING

The Contractor shall provide for the collection and reporting of statistical information on a weekly, monthly, quarterly and as needed basis.

11.1. WEEKLY REPORTS

The weekly reporting requirements are presented below in Table 31.

Table 31 - Weekly Reporting Requirements

Req. #	Description
31-1.	[STATUS REPORT]- The Contractor shall produce a weekly Change Request Status Report that contains detail on the status of Change Requests (CRs) including but not limited to the number of change requests opened/closed and how closed (fixed, deleted, re-assigned).
31-2.	[STATUS REPORT]- The Contractor shall submit to the HUD OIG ISD Security Manager a weekly Security Activity Status Report (and cumulative for the year) that includes the following: 1) Number of incidents; 2) Seriousness of the incidents; 3) Number of hours to resolve; 4) If any proprietary data was compromised; 5) If any exogenous data was compromised.
31-3.	[STATUS REPORT]- The Contractor shall submit to the HUD OIG ISD Security Manager a weekly Security Status Report that includes but is not limited to the following: accomplishments for reporting period; plans for next reporting period; issues and risks, scheduled milestones; computer system incidents reported to HUD OIG ISD; computer system incidents reported to US CERT; Network incidents reported to HUD OIG ISD; POAM items completed;

Req. #	Description
31-4.	[STATUS REPORT]- The Contractor shall submit to the HUD OIG ISD COTR a weekly status report that identifies: accomplishments for the reporting period, projected tasks for the coming week and person assigned to that task.
31-5.	[STATUS REPORT]- The Contractor shall provide a weekly status report to the HUD OIG ISD Operations/Maintenance POC that reflects: server time up and virtualization performance measures.
31-6.	[STATUS REPORT]- The Contractor shall report to the HUD OIG ISD Operations/Maintenance POC in a weekly report the results of network monitoring, including the status and performance of the WAN, LANs and DCE.

11.2. MONTHLY REPORTS

The monthly report requirements are presented below in Table 32.

Table 32 - Monthly Reporting Requirements

Req. #	Description
32-1.	[STATUS REPORT]- The Contractor shall submit, within 10 business days of the end of each month, a Monthly Management Report that includes but is not limited to the following information: 1) Activities performed during the month, 2) Summary of the weekly Security Activity Reports, 3) Summary of the weekly Change Request reports, 4) SLA metrics and supporting documentation, 4). accomplishments for reporting period, 5) plans for next reporting period, 6) risks/issues/problems, and 6) cumulative scheduled milestones by actual and scheduled completion date and status. This Management Report shall be submitted with the invoice for the same reporting period.[
32-2.	[STATUS REPORT]- The Contractor shall submit, within 10 business days of the end of each month, a fiscal report that includes but is not limited to actual and cumulative expenditures for the reporting period, by CLIN, (OMB-300 Monthly Reporting for IT-Dashboard). This may be included as a separate page with the Monthly Management Status Report. This Fiscal Report shall be submitted with the invoice for the same reporting period.
32-3.	[STATUS REPORT]- The Contractor shall provide, within 10 business days of the end of each month, a monthly status report to the HUD OIG ISD Security Officer that includes but is not limited to the following information: accomplishments during reporting period; plans for next reporting period; risks/issues; milestones by actual and scheduled completion date and status computer system incidents reported to HUD OIG ISD and reported to US CERT; network incidents reported to HUD OIG ISD and reported to US CERT; Security-based POAM items, criticality, scheduled and actual date of closure and status.
32-4.	[STATUS REPORT]- The Contractor shall provide to the HUD OIG ISD Help Desk POC, within 10 business days of the end of each month, a

Req. #	Description
	status report reflecting service requests to the Help Desk for assistance by performance metrics (e.g., number of requests per hour/per day; number of requests by HUD OIG ISD provided category).
32-5.	[STATUS REPORT]- The Contractor shall provide to the HUD OIG ISD Functional (e.g., Operations/Maintenance, Security, Help Desk) POCs, within 10 business days of the end of the month, a report that includes but is not limited to each applicable SLA, its threshold, and the actual measure for that SLA. The report shall specify which SLA's have been met and which have not, including the percentage of the total SLA's that have been met/not met. The report shall also specify the percentage of SLA's that have fallen below/above their applicable threshold.
32-6.	[STATUS REPORT]- The Contractor shall provide to the Operations and Maintenance HUD OIG ISD POC, within 10 business days of the end of each month, Operations/Maintenance Status reports including but not limited to the reactive and proactive operations and maintenance activities performed.
32-7.	[STATUS REPORT]- The Contractor shall, within 10 days of the end of the month, provide a monthly status report to the HUD OIG ISD POC including but not limited to a summary of the number of change requests opened/closed and how closed (fixed, deleted, re-assigned).

11.3. QUARTERLY REPORTS

The quarterly report requirements are presented below in Table 33.

Table 33 - Quarterly Reporting Requirements

Req. #	Description
33-1	[STATUS REPORT]- The Contractor shall, within 10 days of the end of the quarter, provide to HUD OIG ISD a Quarterly Management Report package that includes but is not limited to the following information: 1) Activities performed during the quarter, and 2) SLA metrics and supporting documentation.
33-2	[STATUS REPORT]- The Contractor shall, within 10 days of the end of the quarter, identify to HUD OIG ISD, in writing, on a quarterly basis, the specific support personnel and the backup personnel for all systems. Any changes to these assignments shall be provided verbally to the government immediately and furnished in writing within eight (8) hours.
33-3	[STATUS REPORT]- The Contractor shall provide to the HUD OIG ISD quarterly SLA Reports no later than 10 business days prior to the quarterly scheduled meeting. The SLA Reports shall include but is not limited to: target vs. actual; number met; number not met; rationale for not meeting target; expected date for meeting target.

11.4. ANNUAL REPORTS

The annual reporting requirements are presented below in Table 34.

Table 34 - Annual Reporting Requirements

Req. #	Description
34-1	[STATUS REPORT]- The Contractor shall provide to the Government, 60 days after Contract signing, and on an annual basis, no later than Feb 1 of each subsequent year an Inventory Report of all Government furnished equipment (GFE). The Inventory Report shall identify all equipment purchased during the current inventory period.
34-2	The Contractor shall provide to the Government a current inventory of all IP compliant devices and technologies no later than April 30th of each year for submission to OMB no later than June 30th. (OMB 05-22).

11.5. MEETING REQUIREMENTS

The meeting requirements are presented below in Table 35.

Table 35 - Meeting Requirements

Req. #	Description
35-1	[MEETING]- The Contractor shall provide a monthly management briefing to the HUD OIG ISD. The purpose of this briefing is to walk-through the monthly status report including financial information; to describe program risks and issues; and to respond to HUD OIG ISD questions and concerns. It is expected that the briefing will be provided by the Contractor's Project Manager.
35-2	[MEETING]- The Contractor shall participate in management reviews, as required by the HUD OIG ISD.
35-3	[MEETING]- The HUD OIG ISD will request unscheduled technical meetings with the Contractor at the HUD OIG ISD's discretion.
35-4	[MEETING]- The Contractor shall provide a quarterly technical briefing to the HUD OIG ISD. The purpose of this briefing is to inform the HUD OIG ISD of risks and mitigation strategies; and to raise technical issues not previously identified.
35-5	[MEETING]- The Contractor shall invite the HUD OIG ISD POCs to all Contractor's status meetings in keeping with the concept of one uniform team.

12.0 MANAGEMENT REQUIREMENTS

The HUD OIG ISD intends to reduce risk and uncertainty through its project management activities. HUD OIG ISD expects the project management activities to create repeatability, reliable performance and standardization. As such it expects the Contractor to plan, organize and control all activities, tasks, and resources. In addition to its operations and maintenance activity, the HUD OIG ISD anticipates having multiple projects each having a limited and defined duration. The Contractor also will be responsible for planning, organizing and controlling these projects.

12.1 PROJECT MANAGEMENT REQUIREMENTS

The project management requirements are provided below in Table 36.

Table 36 – Project Management Requirements

Req. #	Description
36-1.	The Contractor shall manage the contract line items as required to support the DCE.
36-2.	The Contractor shall manage purchases of equipment and services and other direct charges (ODCs) in accordance with the FAR.
36-3.	The Contractor shall manage operations, projects, resources, and budgets utilizing an accepted project management methodology such as that promulgated by the Project Management Instute (PMI).
36-4.	The Contractor shall collect data on requested processing activities, and shall generate and submit to HUD OIG ISD ad hoc reports requested by the HUD OIG ISD. The period of performance for generating and submitting the requested report will be negotiated between the Contractor and HUD OIG ISD at the time of request.

12. 2 CONTRACT MANAGEMENT REQUIREMENTS

Contract management focuses on such things as project management, change control, baselines, technology, performance, quality assurance, and contractor resources. The intent of HUD OIG ISD is to manage the contract and not the people by focusing on the quality and timeliness of results.

Contract performance will be managed through the use of service level agreements (SLAs) that define the HUD OIG ISD expectations of the Contractor's performance for each component of service delivery. In addition to the quantitative SLAs , the HUD OIG ISD will include as performance the timely delivery and acceptance of plans, reports, and other documents required by the contract. The contract management requirements are provided below in Table 37.

Table 37 – Contract Management Requirements

Req. #	Description
37-1.	The Contractor shall adhere to all the targets identified in the associated Service Level Agreement (SLA).
37-2.	The Contractor shall collect data on requested processing activities, and shall generate and submit to HUD OIG ISD ad hoc reports requested by the HUD OIG ISD. The period of performance for generating and submitting the requested report will be negotiated between the Contractor and HUD OIG ISD at the time of request.
37-3.	The Contractor shall document, and provide to HUD OIG ISD, a methodology for addressing those areas where performance levels are not being met.

SEE ATTACHED TECHNICAL PERFORMANCE INDEX